

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

IN RE EQUIFAX INC. SECURITIES
LITIGATION

Consolidated Case No.
1:17-cv-03463-TWT

**CONSOLIDATED CLASS ACTION COMPLAINT FOR
VIOLATIONS OF THE FEDERAL SECURITIES LAWS**

TABLE OF CONTENTS

	<u>Page</u>
I. PRELIMINARY STATEMENT	2
II. PARTIES	10
A. Lead Plaintiff.....	10
B. Defendants.....	10
1. Equifax, Inc.....	10
2. Individual Defendants.....	12
III. JURISDICTION AND VENUE.....	13
IV. SUMMARY OF THE FRAUD	13
A. Equifax’s Business is to Collect and Sell Sensitive Personal Information About Global Consumers.....	13
B. Defendants Knew that Securing the Information Equifax Collected Was Critical to the Company’s Business.....	16
C. Defendants Issue Statements Touting Cybersecurity, Compliance with Data Protection Laws and Regulations, and Certifying the Integrity of Equifax’s Internal Controls	24
1. Defendants Touted the Security of Equifax’s Data Systems’ and The Company’s Efforts to Protect Consumer Information	25
2. Defendants Assured Investors That Equifax Zealously Complied with Data Protection Laws, Regulations, and Industry Best Practices.....	27

3.	Defendants Assured Investors That Equifax Had Adequate Internal Controls	28
D.	In Truth, Equifax Failed to Adequately Secure and Protect Sensitive Consumer Information.....	29
E.	Equifax Ignored Numerous Warnings That Its Data Protection Measures Were Inadequate to Protect Sensitive Information.....	33
1.	In 2013 and 2014 Equifax Experiences Breaches Due to Inadequate Cybersecurity.....	33
2.	KPMG Flags Equifax’s Unsafe Encryption Practices	35
3.	Equifax’s “Attack Surface” Becomes Too Large to Defend	35
4.	The W2Express Breach.....	36
5.	Equifax Is Warned Repeatedly About Patching Deficiencies.....	38
6.	Throughout the Class Period Security Researchers Continue to Warn Equifax About Serious Cybersecurity Deficiencies, but These Warnings are Ignored.....	40
7.	The LifeLock Breach	43
8.	The TALX Breach	43
9.	Equifax Hires Mandiant, But Ignores Its Advice	46
F.	Equifax’s Failure to Implement Basic Data Protection Measures Leads to The Massive Data Breach.....	47
G.	The Truth About Equifax’s Inadequate Cybersecurity Is Finally Revealed to Investors	61
1.	Revelations Affecting Trading on September 8, 2017	62
2.	Revelations Affecting Trading on September 11, 2017	68

3.	Revelations Affecting Trading on September 13, 2017	72
4.	Revelations Affecting Trading on September 14, 2017	77
5.	Revelations Affecting Trading on September 15, 2017	80
H.	Post-Class Period Developments	81
1.	Smith Departs the Company Without Severance	81
2.	Defendants Have Now Admitted that There Were Numerous Serious Deficiencies in Equifax’s Data Security Posture	82
3.	Equifax’s Data Protection Measures Are Severely Criticized by Experts, Lawmakers, and Others	87
4.	Equifax’s Business Continues to Experience Significant Harm As a Result of the Data Breach.....	93
I.	Equifax’s Data Protection Measures Were Grossly Inadequate, and Failed to Meet Either Basic Industry Standards or Applicable Legal Requirements	94
1.	Equifax Failed to Implement an Adequate Patch Management Process and Routinely Failed to Address Known Vulnerabilities	95
2.	Equifax Failed to Encrypt Sensitive Data.....	100
3.	Equifax Failed to Implement Adequate Authentication Measures	103
4.	Equifax Failed to Adequately Monitor Its Networks	107
5.	Equifax Allowed Sensitive Data to be Easily Accessed On Public-Facing Servers and Also Failed to Partition It	109
6.	Equifax Inappropriately Relied on Outdated and Obsolete Security Systems and Software.....	111

7.	Equifax Allowed Its “Attack Surface” to Balloon.....	114
8.	Equifax Allowed Unused Data to Accumulate on Vulnerable Systems and Failed to Dispose of Unneeded Data	115
9.	Equifax Failed to Restrict Access to Sensitive Data	116
10.	Equifax Management Failed to Foster a Strong Security Culture and Ensure Adequate Training of Security Personnel.....	118
11.	Equifax Failed to Perform Adequate Security Reviews	122
12.	Equifax Failed to Develop an Adequate Data Breach Plan...	124
V.	ADDITIONAL ALLEGATIONS OF SCIENTER	126
VI.	DEFENDANTS’ MATERIALLY FALSE AND MISLEADING STATEMENTS	139
A.	Defendants’ Materially False and Misleading Statements Concerning Equifax’s Cybersecurity and the Company’s Efforts to Protect Consumer Information.....	139
1.	False and Misleading Statements Published on the Equifax Website	139
2.	Equifax’s SEC Filings.....	146
3.	Equifax Investor Conferences and Presentations	150
B.	Defendants’ Materially False and Misleading Statements Concerning Equifax’s Compliance with Data Protection Laws, Regulations, and Industry Best Practices	160
1.	False and Misleading Statements Published on the Equifax Website	160
2.	Equifax’s SEC Filings.....	162

C.	Defendants’ False and Misleading Statements Concerning Equifax’s Internal Controls	166
VII.	LOSS CAUSATION	168
VIII.	PRESUMPTION OF RELIANCE	176
IX.	INAPPLICABILITY OF THE STATUTORY SAFE HARBOR.....	177
X.	CLASS ACTION ALLEGATIONS.....	177
XI.	COUNTS	180
XII.	PRAYER FOR RELIEF	185
XIII.	JURY DEMAND.....	185

Lead Plaintiff Union Asset Management Holding AG (“Union”) brings this action under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934 (the “Exchange Act”) on behalf of itself and all other similarly situated purchasers of the securities of Equifax, Inc. (“Equifax” or the “Company”) from February 25, 2016 through September 15, 2017, inclusive (the “Class Period”).

Lead Plaintiff alleges the following upon personal knowledge as to itself and its own acts, and upon information and belief as to all other matters. Lead Plaintiff’s information and belief is based on, among other things, the independent investigation of Court-appointed Lead Counsel Bernstein Litowitz Berger & Grossmann LLP. This investigation included, among other things, a review and analysis of: (i) Equifax’s public filings with the SEC; (ii) public reports and news articles; (iii) research reports by securities and financial analysts; (iv) transcripts of Equifax’s investor calls; (v) economic analyses of securities movement and pricing data; (vi) consultations with relevant experts; and (vii) other publicly available material and data identified herein. Lead Counsel’s investigation into the factual allegations contained herein is continuing, and many of the facts supporting the allegations contained herein are known only to the Defendants or are exclusively within their custody or control. Lead Plaintiff believes that further substantial evidentiary support will exist for the allegations contained herein after a reasonable opportunity for discovery.

I. PRELIMINARY STATEMENT

1. This case is about the massive gulf between what Defendants said about cybersecurity and what they actually did. For example, during the Class Period, Equifax stated:

As a *trusted steward* of consumer and business information, Equifax employs *strong data security and confidentiality standards* on the data we provide and on the access to that data. We maintain a highly sophisticated data information network that includes *advanced security, protections and redundancies*.¹

Equifax also stated that the Company:

[P]rotect[s] the privacy and confidentiality of personal information about consumers. . . . Safeguarding the privacy and security of information, both online and offline, is *a top priority for Equifax*.

And Equifax's former CEO, Defendant Smith, reassured investors that:

Data security is . . . top of mind. . . . [I] feel like *we're in really good shape*.

2. Contrasting these statements are analyses of the realities of Defendants' cybersecurity during the Class Period. For instance, the Institute for Critical Infrastructure Technology, a prominent cybersecurity think tank, concluded:

A breach of Equifax systems was *inevitable*. . . [B]ecause *the C-suite exhibited . . . a lack of cyber-hygiene, and a disregard for information security training and qualified personnel*.

Likewise, a November 2017 *Forbes* article quoted cybersecurity expert

¹ Unless otherwise noted, any emphasis in quotations contained in this Complaint is added.

Wes Moehlenbruck's conclusion that:

The real problem was a very poor focus on information security at the highest levels of the company – what we call C-level.

3. Defendants Equifax, Smith, Gamble, Ploder and Dodge made numerous additional false and misleading statements and omissions about the Company's efforts to safeguard the highly sensitive personal information at the core of the Company's business, the vulnerability of its internal systems to a cyberattack, and its compliance with applicable data protection laws and cybersecurity best practices. As detailed herein, and contradicting its public disclosures, Equifax failed to take basic steps to protect the Company from intrusions and data theft, and ignored warnings from consultants, independent security researchers, and others that its cyberdefenses were woefully inadequate to protect the exceedingly valuable information the public had entrusted to it. As a result of Defendants' misconduct, hackers penetrated Equifax's systems in March of 2017, resulting in the largest and most devastating security breach in American history (the "Data Breach"). Personal information belonging to more than 148 million Americans – half the country's adult population – was compromised in the attack. However, even when, in July 2017, Equifax discovered that its highly sensitive databases had been compromised Defendants concealed this crucial information from investors and the public. Finally, beginning on September 7, 2017, Equifax began to disclose facts revealing

the profound inadequacy of the Company's cybersecurity, causing Equifax's stock price to tumble and wiping out billions in shareholder value.

4. Equifax's business consists almost exclusively of collecting, aggregating and selling the sensitive personal data of individual consumers. Equifax repeatedly acknowledged that maintaining such information on its computer networks made it a highly-visible target for hackers and other criminals seeking to obtain and leverage that information.

5. Defendant Smith, Equifax's former CEO, personally acknowledged the risks associated with the Company's possession of massive amounts of consumer data and told investors that the Company's ability to protect its database "it's my number one worry, obviously." Similarly, Defendant Dodge, Equifax's Director of Investor Relations, assured investors that, given the importance of data security to Equifax, unlike other businesses that sell "hammers," if Equifax had a data breach, "we're not in too good a shape out of that, right? So data security and how we go about ensuring that is something we spend a lot of time and effort on."

6. In statements like those quoted above, Defendants sought to reassure investors and the public about Equifax's ability to protect the personal information of hundreds of millions of consumers and repeatedly touted the Company's commitment to, and the strength and integrity of, its cybersecurity program.

7. Those statements, and the many like them detailed in this Complaint, were false. As a result of Equifax's disastrously inadequate cybersecurity, investors

have suffered a massive decline in the value of their Class Period purchases of Equifax securities. The stunning reality of Equifax's cybersecurity problems came to light beginning on September 7, 2017, when Equifax disclosed the Data Breach in which criminal hackers stole the social security numbers, birth dates, addresses, and drivers' license numbers of over 140 million Americans.

8. In the days that followed, additional information revealed the depth of Equifax's fraudulent statements about cybersecurity. As the news concerning the true state of Equifax's cybersecurity became known, the price of Equifax's stock dropped precipitously. Over the six trading days following the September 7, 2017 disclosure of the Data Breach, when its magnitude and root causes became known, Equifax's stock price declined by a total of 25%, or \$30.25 per share, wiping out \$3.6 billion of the Company's market capitalization.

9. The market was rightly shocked that Equifax's inadequate cybersecurity had allowed criminal hackers to access and steal the "personal information" ("PI") of 148 million Americans through what amounted to an open door. The information stolen is incredibly valuable, and will allow criminals who obtained it to engage in identify theft, filing of fraudulent tax returns, and other damaging activity.

10. The Data Breach and its aftermath revealed that Equifax's security efforts were impossibly flawed. Rather than acting as a "trusted steward" of the information entrusted to it as a key player in the United States and international

credit process, it became clear that Equifax did not properly store and protect the sensitive data it collected and trafficked in. Indeed, as explained in detail in Section IV(I), Equifax wholly failed to comply with applicable laws, regulations, and industry standards governing cybersecurity security. Among other things:

- Equifax failed to implement a process to ensure that its software was updated and “patched,” and used obsolete or outdated software;
- Equifax failed to implement adequate encryption measures to protect sensitive information in its custody;
- Equifax failed to implement adequate authentication measures – proper passwords and “PINs” – to ensure that the process for accessing its networks would prevent intrusions;
- Equifax failed to adequately monitor, and establish mechanisms for monitoring, its networks and systems to detect intrusions;
- Equifax stored PI so that it was easily accessible and on public facing networks; and
- Equifax failed to set a “tone at the top” that promoted data security within the Company and failed to ensure that employees responsible for data security were qualified and adequately trained.

11. Perhaps most troubling, Defendants knew or should have known about these deficiencies, demonstrating that their Class Period statements were made with scienter – knowingly or with reckless disregard for the truth. The Company had suffered numerous prior intrusions and was repeatedly warned by consultants it had hired that it had fundamental cybersecurity weaknesses that needed to be remedied.

12. As a result of these systemic failures, Equifax’s systems were the subject of multiple hacking intrusions in 2013, 2014, 2016, and in early 2017. For

example, the 2016 hack of Equifax's W2Express service was very serious and resulted in a significant settlement that required Equifax to change its password authentication standards, but Equifax failed to implement those changes before the Data Breach. Equifax's inadequate authentication standards also made a February 2017 breach of its Workforce Solutions business (formerly known as "TALX") possible. As was revealed after the Data Breach, preceding and continuing into the Class Period, multiple security researchers also discovered material security weaknesses in Equifax's websites and alerted the Company. These include a serious "cross-site scripting" vulnerability that had been pointed out to Equifax in March 2016 but remained unresolved until after the Data Breach. Equifax and the Individual Defendants repeatedly ignored these warnings and uniformly failed to remedy these weaknesses.

13. Equifax failed to heed the private advice of its consultants and cybersecurity experts. For example, an audit conducted in 2016 by Deloitte was "ignored" by Equifax's senior management. Following the 2016 W2Express breach the Company hired Mandiant in early 2017 to conduct a cybersecurity audit. Smith was personally responsible for overseeing that security audit and Mandiant's recommendations would have prevented the Data Breach, but Equifax (and Smith personally) ignored them.

14. These prior incidents and warnings put Defendants on clear notice of the problems with Equifax's security management, procedures and infrastructure.

The same cybersecurity problems that enabled the prior hacks and that were identified by the Company's experts also enabled the Data Breach. As investors learned in the days following disclosure of the Data Breach, the devastating incident could have been easily prevented if Equifax had just updated the Apache Struts software the Company used to run its consumer dispute portal website. That software vulnerability was widely publicized by no later than March 7, 2017, and the software's developer made a "patch" available the next day. In news articles, government alerts, and industry notices, both the vulnerability and the patch were described as "critical." Indeed, on March 7 and March 9, 2017, respectively, the patch was the subject of an alert by the U.S. Department of Homeland Security ("DHS") and then an *email sent by DHS directly to Equifax*, instructing it to update the Apache Struts software and patch the security weakness. On March 10, a division of the Department of Commerce published a similarly severe notice. Equifax failed to heed any of these warnings.

15. Given the "open door" Equifax had provided to hackers, beginning in March 2017, criminals first discovered the weakness and invaded Equifax's network. As a direct result of Equifax's failure to implement adequate data protection measures, even when urged to do so by its consultants, the hackers remained present in the Company's systems, undetected by Equifax, for approximately five months, during which they stole the PI of the 148 million Americans. Equifax claims to have first discovered the intrusion on July 29, and

shut down access to the compromised parts of its network. But this was only well after the unencrypted data, stored on a public-facing server, was stolen. Even after discovering the intrusion and alerting the authorities to the Data Breach on August 2, 2017, Defendants waited over five weeks to disclose it to investors and the public on September 7, 2017.

16. Thus, notwithstanding Defendants' repeated statements concerning their commitment to cybersecurity, the integrity of the Company's data protection measures and their compliance with applicable law and standards governing data security, Equifax failed to engage in the simple step of updating that software. All of the warnings and bad outcomes privately communicated to Equifax by its advisors, consultants, and others, came true. Defendant Smith would later admit that the reason why the Apache Struts vulnerability was not patched was because *one person* at the Company was responsible for all software updates and patching. Since the Data Breach, Equifax also replaced its outdated and obsolete "scanners," and admitted that it had run vulnerability scans on only parts of its database, omitting critical portions of its infrastructure, including those hacked in the Data Breach. This alone is an admission that the Company's representations about cybersecurity, compliance with industry standards and Equifax's internal controls were false. Moreover, severity of the problems underlying the Data Breach make clear that not only did Defendants utterly fail at actually implementing an adequate cybersecurity

defense, they did *not even make a good faith effort* to protect the PI of 148 million people.

17. The end result of this has been a parade of terribles for Equifax’s investors, with Smith admitting that “obviously a breach of this magnitude would not have occurred if everything was – was in place.” That apology has done nothing to restore the \$3.6 billion in shareholder value wiped out following the Data Breach.

II. PARTIES

A. Lead Plaintiff

18. Lead Plaintiff Union Asset Management Holding AG is the parent holding company of the Union Investment Group. The Union Investment Group, based in Frankfurt-am-Main, Germany, was founded in 1956, and is one of Germany’s leading asset managers for retail and institutional clients with more than €292 billion assets under management as of December 31, 2017. As set forth in the certification filed with this Court (ECF No. 11-6), Union’s funds purchased Equifax common stock during the Class Period and were damaged by Defendants’ conduct as alleged herein.

B. Defendants

1. Equifax, Inc.

19. Defendant Equifax, Inc. (“Equifax” or “the Company”) is a Georgia corporation headquartered in Atlanta, Georgia. Equifax is one of the three largest credit reporting agencies in the world, and participates both in the business-to-

business sector and the direct-to-consumer sector by collecting and selling data on more than 820 million consumers and business globally.

20. The Company operates through four primary segments: U.S. Information Solutions (USIS); International; Workforce Solutions; and Global Consumer Solutions:

a. The USIS business segment provides three general categories of products and services to businesses: Online Information Solutions, Mortgage Solutions, and Financial Marketing Services. These services include selling products focused on consumer and commercial credit reporting, identity management, and fraud detection, as well as credit decisioning software services.

b. Equifax's International operating segment includes the Company's Asia Pacific, Europe, Latin America, and Canada business units.

c. Equifax's Workforce Solutions segment operates through two primary business units: Verification Services and Employer Services. Verification Services enables third-party verifiers, including governmental agencies, to verify an individual's employment status and income information. Employment Services aids businesses' human resources function in managing a variety of employment tax matters and unemployment claims management. Equifax's Workforce Solutions' services utilize the Company's Work Number database, the Company's primary repository of employment and income data.

d. Equifax's Global Consumer Solutions segment is its direct-to-consumer business, and provides consumers with products enabling them to protect and monitor their credit and identity, including the TrustedID consumer credit protection service.

2. Individual Defendants

21. Defendant Richard F. Smith ("Smith") is the former Chief Executive Officer ("CEO") and Chairman of the Board of Directors of Equifax. Smith became CEO and Chairman on December 15, 2005 and held those positions throughout the Class Period until his resignation from both positions on September 26, 2017.

22. Defendant John W. Gamble ("Gamble") is the Corporate Vice President and Chief Financial Officer ("CFO") of Equifax. Gamble joined Equifax as its CFO on May 21, 2014 and held that position throughout the Class Period.

23. Defendant Rodolfo O. Ploder ("Ploder") is the President of Equifax's Workforce Solutions operating segment. Ploder assumed the role of President in November 2015 and held that position throughout the Class Period. Ploder joined Equifax in February 2004.

24. Jeffrey L. Dodge ("Dodge") is the Senior Vice President of Investor Relations at Equifax. Dodge assumed this role in May 2002.

25. Defendants Smith, Gamble, Ploder, and Dodge are collectively referred to hereinafter as the "Individual Defendants" and, together with Equifax, the "Defendants."

III. JURISDICTION AND VENUE

26. The claims asserted herein arise under and pursuant to Sections 10(b) and 20(a) of the Exchange Act, 15 U.S.C. §§ 78j(b) and 78t(a), and Rule 10b-5, 17 C.F.R. § 240.10b-5. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331 and Section 27 of the Exchange Act, 15 U.S.C. § 78aa.

27. Venue is proper in this District pursuant to Section 27 of the Exchange Act and 28 U.S.C. § 1391(b), as Equifax's principal executive office is located within this District at 1550 Peachtree Street, N.W. Atlanta, Georgia 30309, and many of the acts and practices complained of herein occurred in substantial part in this District.

28. In connection with the acts alleged herein, Defendants, directly or indirectly, used the means and instrumentalities of interstate commerce, including, but not limited to, the mails, interstate telephone communications, and the facilities of the national securities markets.

IV. SUMMARY OF THE FRAUD

A. Equifax's Business is to Collect and Sell Sensitive Personal Information About Global Consumers

29. Equifax is one of the three major credit-reporting bureaus in the United States, and, throughout the Class Period, characterized itself as a "leading global provider of information solutions." Equifax's business is to collect, maintain, and sell a wide variety of personal data about the world's consumers and employees. As Equifax explained in filings with the SEC, "Our products and services are based on

comprehensive databases of consumer and business information derived from numerous sources of credit, including financial assets, telecommunications and utility payment, employment, income, public record, demographic and marketing data.” In even starker terms, Equifax told investors, “Data is at the core of our value proposition.” During the Class Period, Equifax collected and maintained sensitive personal data relating to more than 820 million consumers and 91 million businesses worldwide.

30. Traditionally, credit bureaus collect and sell credit data – comprised of Social Security numbers, addresses, employment history, detailed balance and repayment information for financial accounts, and other highly sensitive information – to lenders. Credit bureaus acquire this information from banks, credit card issuers, mortgage lenders, and other financing companies, merchants, and creditors. They then sell that information to other potential creditors who are interested in understanding the credit profile of a particular consumer.

31. For instance, when a consumer applies for a credit card, the information the consumer supplies to the credit card company – including Social Security numbers, addresses, and other personal identifiers – is forwarded to the credit bureau. The credit card company will then receive certain information concerning the applicant’s credit history. If the credit card company issues a card to the applicant it will then continue to report the consumer’s payment history to the credit bureaus. Consumers cannot prevent credit bureaus from collecting and maintaining

sensitive personal information about them, and, with few, very limited exceptions, cannot prevent those bureaus from selling that personal information to third parties.

32. When Smith became Equifax's CEO in 2005, Equifax was a traditional credit bureau, focused primarily on selling credit data, and was growing at an organic rate of 1% to 2% per year. As Smith explained in an August 2017 speech at the University of Georgia, he sought to dramatically accelerate Equifax's growth by transforming it into a "global data-analytics company." To do so, Smith greatly expanded the breadth and depth of consumer data that Equifax collected and monetized to include, among other things, payroll and tax data, and detailed information about consumer spending and behavior.

33. In large part, Equifax accomplished this rapacious acquisition of new data by buying other companies. For instance, in 2007, Equifax acquired TALX (renamed Equifax Workforce Solutions in 2012), which maintained a user-paid employment verification database called "The Work Number." The Work Number contains data derived from employees' income and employment records, including years' worth of weekly salary data, unemployment claims, and health provider and insurance data. The Work Number database includes these data for nearly half of all American workers, which was culled from more than 7,000 employers, including 75% of the Fortune 500 companies. The Company sells data maintained in the Work Number to businesses, governments, and institutions for purposes of, among other things, verifying employment and salary history of job applicants, and evaluating

eligibility for government benefits. Notably, after the Company acquired this database and began working to expand it, Equifax issued statements on its website reassuring the public that “[a]s W-2 data is sensitive and subject to federal regulations, *every precaution is taken to ensure both security and accuracy.*”

34. Likewise, during Smith’s tenure, Equifax acquired vast troves of data on overseas consumers in acquiring TDX Group, the United Kingdom’s largest debt placement service, and Veda Group Ltd., an Australian credit information and analytics company, among others. Equifax also launched an identity protection business by acquiring companies like TrustedID and ID Watchdog, and sold data breach solution products to companies affected by cyberattacks.

35. As Smith explained in a 2011 interview, Equifax’s push into ever wider and more detailed data sets turned Equifax into a business that housed “\$12 trillion of consumer wealth data.” “Without us,” Smith stated, “you wouldn’t have global commerce as you know it today.”

B. Defendants Knew that Securing the Information Equifax Collected Was Critical to the Company’s Business

36. As Defendants were well aware, the data Equifax amassed was highly sensitive and concerned the most intimate and personal aspects of consumers’ and employees’ lives. Indeed, in a 2012 interview, former Equifax Chief Information Officer David Webb (who would later be terminated in connection with the Data Breach) acknowledged, “*We know more about you than you would care for us to know* The morality question [of aggressive data mining] is another discussion.

But we have the technology to do this, and if it's legal, we should.” As discussed above, Equifax amassed detailed information about consumers' Social Security numbers, addresses, birthdays, driver's license information, credit card information, loans, bills, payment history, employment records, insurance information, and more.

37. Cybersecurity experts, regulators, and legislators have emphasized the extraordinary value and sensitivity of the information Equifax acquired, collected and sold. For instance, with respect to Social Security numbers, addresses, birthdays, and other information exposed in the Data Breach, Brian Vecci, a cybersecurity expert at Varonis Systems Inc., told the *Wall Street Journal* in September 2017, “That's the information you would need to set up a bank account or change your phone number – it's crazy how valuable this kind of data is.” Vecci further stated that this information, which comprises the information consumers provide to obtain their credit scores, “is like the keys to the digital kingdom. If I have all that, I can probably walk to a bank and get a mortgage with it.” Likewise, in an October 4, 2017 Senate Banking Committee hearing, Senator Sherrod Brown characterized the information maintained by Equifax – and specifically the information exposed in the Data Breach – as “the most private information” about American consumers and a “gold mine for hackers.”

38. Defendants understood that given the sensitivity of the personal data the Company maintained, Equifax's failure to adequately protect those data would wreak havoc on its customers, on consumers all over the world, and, therefore, on

Equifax's business. Equifax's profitability was dependent on what the Company touted in its SEC filings as its "reputation as a trusted steward of information," which those filings characterized as among "the principal competitive factors affecting [its] markets," and on the uniqueness of the data it sold. Accordingly, as Equifax repeatedly acknowledged, safeguarding those data was fundamental to the Company's business. In its SEC filings throughout the Class Period, Equifax acknowledged that cyberattacks posed a material threat to its business, stating:

[W]e collect and store sensitive data, including intellectual property, proprietary business information and personally identifiable information of our customers, employees, consumers and suppliers, in data centers and on information technology networks. ***The secure and uninterrupted operation of these networks and systems, and of the processing and maintenance of this information, is critical to our business operations and strategy.***

39. Equifax further acknowledged in its SEC filings that the Company was a high-value target of cybercriminals; that it was imperative that Equifax develop, continuously monitor, and update, a sophisticated security infrastructure; and that a failure to safeguard the information in the Company's possession could trigger a host of disastrous financial consequences for the Company:

We are regularly the target of attempted cyber and other security threats and must continuously monitor and develop our information technology networks and infrastructure to prevent, detect, address and mitigate the risk of unauthorized access, misuse, computer viruses and other events that could have a security impact 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.

40. Likewise, a September 7, 2017 press release announcing the Data Breach quoted Smith as conceding that the hack “strikes at the heart of who we are and what we do.” And in October 5, 2017 testimony before the House Financial Services Committee, Smith acknowledged that Equifax “is a data company . . . data security is the number one risk we have.” On Equifax’s third quarter 2017 earnings call, after the Data Breach was disclosed and Smith departed the Company, interim Equifax CEO Paulino Barros (“Barros”) acknowledged that “Equifax’s historic success was built on the trust our customers placed in us to help them solve difficult business problems with unique data and analytical assets. *This was, of course, predicated on their trust [in] our IT and data security capabilities.*”

41. The importance of data security to Equifax’s financial well-being, and indeed its continued existence, was also widely discussed within the Company, including during the Class Period. As *Bloomberg* reported in a September 2017 article, “In the corridors and break rooms of Equifax Inc.’s giant Atlanta headquarters, employees used to joke that their enormously successful credit reporting company was just one hack away from bankruptcy.”

42. Equifax and its executives knew that not only was safeguarding the data the Company maintained essential to its financial well-being, Equifax was also affirmatively required by law to implement rigorous cybersecurity defenses.

Because consumers do not opt-in to the credit monitoring process and have little control over the manner in which data aggregators like Equifax store and disseminate their personal information, federal, state, and foreign law protects them by imposing strict duties on those data aggregators to vigilantly safeguard the personal data they amass. As Equifax stated in its SEC filings, the Company is “subject to federal, state and foreign laws regarding the collection, protection, dissemination and use of non-public personal information we have in our possession.”

43. These laws codify public expectations that companies like Equifax, which collect the most personal and private information about consumers, will implement correspondingly secure and sophisticated cybersecurity measures to protect those data. As Senator Brown explained, consumers “should have been able to expect the company that gathers the most private information about them would have state-of-the-art protections for that information. A gold mine for hackers should be a digital Fort Knox when it comes to security.”

44. As discussed in further detail below, the Financial Services Modernization Act of 1999, more commonly known as the Gramm-Leach-Bliley Act (“GLBA”), requires financial institutions, including credit bureaus like Equifax, to “protect the security and confidentiality” of the personal information they collect by, among other things, “develop[ing], implement[ing], and maintain[ing] a comprehensive information security program” that “contains administrative, technical, and physical safeguards that are appropriate to [the] size and complexity

[of the financial institution], the nature and scope of [its] activities, and the sensitivity of any customer information at issue.” Similarly, the Federal Trade Commission (“FTC”), the agency responsible for enforcing these provisions of the GLBA (known as the “Safeguards Rule”), routinely issues guidance and publishes regulatory decisions explicating in detail the security measures financial institutions must take in order to comply with the Safeguards Rule.

45. Defendants were well aware that Equifax was required to comply with the Safeguards Rule, and that a failure to do so would have severe consequences for the Company. As detailed below, in its Class Period SEC filings, Equifax confirmed that it was subject to GLBA provisions “relating to the physical, administrative and technological protection of non-public personal financial information.”

46. The Federal Trade Commission Act (“FTC Act”) also required Equifax to implement a vigorous cybersecurity defense system. The FTC has brought numerous enforcement actions against entities that store and maintain personal data on the grounds that their failure to maintain a data security regime that appropriately protects those data constitutes an “unfair or deceptive act[] or practice[]” under Section 5 of the FTC Act. The FTC regularly publishes materials specifying the elements of an FTC Act-compliant security program, including regulatory guidance and enforcement decisions.

47. Defendants told investors that they were well aware of the FTC Act’s requirements. The Company’s SEC filings during the Class Period stated: “The

security measures we employ to safeguard the personal data of consumers could also be subject to the FTC Act, and failure to safeguard data adequately may subject us to regulatory scrutiny or enforcement action.”

48. In addition to the Safeguards Rule and the FTC Act’s mandates, at least 16 states have adopted laws requiring businesses to implement and maintain a reasonable data security program that is appropriate to the sensitivity of the information housed in the company’s systems.² Massachusetts regulations, for instance, require that any company that collects or maintains sensitive PI implement a comprehensive, written information security program, which must include encrypting personal information, deploying up-to-date firewall and security patches, granting access to personal information only where it is required to perform job duties, and using secure passwords and unique identifier technologies.

49. Defendants knew that state law, in parallel with federal law, imposed stringent data security requirements on Equifax. In its SEC filings during the Class Period, Equifax acknowledged that:

A majority of states have adopted versions of data security breach laws that require notification of affected consumers in the event of a breach of personal information. Some of these laws require additional data protection measures which exceed the GLB Act data safeguarding requirements. If data within our system is compromised by a breach, we may be subject to provisions of various state security breach laws.

² The states that have adopted data security laws include Arkansas, California, Connecticut, Florida, Indiana, Kansas, Maryland, Massachusetts, Minnesota, Nevada, New Mexico, Oregon, Rhode Island, Texas, and Utah.

50. Finally, Defendants understood that foreign law imposed strict data security requirements on Equifax. Equifax's SEC filings acknowledged that Equifax was subject to: (1) the "comprehensive 1995 European Union Data Protection Directive," which includes a "prohibition on the transfer of personal information from the EU to other countries whose laws do not protect personal data to an 'adequate' level of privacy or security. The [EU] standards for adequacy are generally stricter and more comprehensive than that of the U.S. and most other countries where Equifax operates"; (2) the United Kingdom's Data Protection Act of 1998; and (3) the Canadian Model Code for the Protection of Personal Information, which mandates the implementation of physical, organizational (such as "limiting access on a 'need to know' basis"), and safeguards (such as "the use of passwords and encryption") to protect information in proportion to its sensitivity.

51. In light of the type of data Equifax had in its custody, the importance of data security to the Company's business, and the gravity of its legal obligation to safeguard consumer data, Equifax's senior executives, including Smith, were personally charged with monitoring Equifax's cybersecurity defenses. Smith testified at an October 3, 2017 hearing before the House Energy and Commerce Committee, that he was "in charge of overseeing" Equifax's application and maintenance of cyber-defenses. At that same hearing, Smith testified that he was frequently briefed on Equifax's data security systems: "we would have IT reviews at least quarterly and security reviews at least quarterly. And then you would

augment that on an as-needed basis.” Smith further testified, “I would have active involvement with my general counsel, with the head of security, routinely throughout the year.” In a hearing before the House Financial Services Committee, Smith testified that cybersecurity was at the “[t]op of [the] list” for discussion at Board meetings and that he, along with others members of the Board and Board meeting attendees, received “deep dives” into the Company’s risks and defenses. At that same hearing, Smith testified that the Board’s technology committee separately “would go into details of our security efforts, as well,” and would “make a presentation at every board meeting.”

C. Defendants Issue Statements Touting Cybersecurity, Compliance with Data Protection Laws and Regulations, and Certifying the Integrity of Equifax’s Internal Controls

52. Recognizing that data security is integral to Equifax’s business, and to reassure investors about the Company’s commitment to cybersecurity and the strength of its defenses, Defendants issued a series of materially false and misleading public statements and omissions throughout the Class Period. These statements, and the reasons why they are false and misleading, are detailed comprehensively in Section VI, below. Defendants’ misstatements and omissions misled investors about the measures Equifax took, or failed to take, to secure and protect its internal data systems, and concealed the truth about the vulnerability of those systems to unauthorized intrusions and data theft, including statements in which Defendants continued to tout Equifax’s reputation as a “trusted steward” of consumer data, even

while they knew, but failed to disclose, that those data had been compromised in the Data Breach. Defendants also repeatedly issued false statements assuring investors that Equifax was in compliance with, and was vigilantly working to ensure that it would remain in compliance with, controlling data protection laws, regulations, and industry standards, when in fact, Equifax abjectly failed to comply with them. Finally, Defendants stated that Equifax's internal controls were adequate when in reality, those controls were patently insufficient, inconsistent with the Company's own internal policies and applicable legal, regulatory and industry standards to the point that a massive theft of Equifax's data occurred over a five month period in 2017.

1. Defendants Touted the Security of Equifax's Data Systems' and The Company's Efforts to Protect Consumer Information

53. As discussed above, Defendants issued public statements touting the strength of Equifax's cybersecurity infrastructure, the steps the Company was taking to protect consumer information, and the Company's commitment to cybersecurity.

For instance, during the Class Period, Defendants stated on Equifax's website:

As a *trusted steward* of consumer and business information, Equifax employs *strong data security and confidentiality standards* on the data we provide and on the access to that data. We maintain a highly sophisticated data information network that includes *advanced security, protections and redundancies*.

54. Defendants also stated:

We have built our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to

protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive information we have about businesses. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax.

55. On the same subject, at a May 2016 investor conference, an analyst asked Smith about Equifax’s commitment to cybersecurity particularly in light of news that hackers had accessed W-2 data through an Equifax portal. Smith affirmed the purported strength of Equifax’s data security, stating that the Company “never take[s] for granted our need to continue to innovate around data security. I think we are in a very good position now [I] feel like we’re in really good shape.”

56. At a November 2016 investor conference, Dodge stated that “***data security and how we go about ensuring that is something we spend a lot of time and effort on.***”

57. Defendants also touted Equifax’s role as a “trusted steward” of information as driving the Company’s success. For instance, in an August 2, 2016 presentation to investors, Ploder hailed the success of the Company’s Employment Verification business in both the corporate human resources market and in providing Affordable Care Act eligibility information to the U.S. government, underscoring that Equifax was acting as a “trusted steward of their information.” Indeed, Ploder stated that Equifax’s reputation for vigorous data protection was actually driving the growth of the Work Number database: “That level of trust . . . has allowed us to develop something called the Work Number” Ploder further stated that Equifax acts as “[t]hat trusted steward of information for [human resource departments] to

give us their income and employment records, that in turn then we have an ecosystem of verifiers And *that is what is propelling the growth of our organization.*”

2. Defendants Assured Investors That Equifax Zealously Complied with Data Protection Laws, Regulations, and Industry Best Practices

58. Defendants also issued a series of statements assuring investors that Equifax complied with applicable data protection laws and regulations, and its cybersecurity practices met “or exceed[ed]” industry standards.

59. For example, in its SEC filings throughout the Class Period, Equifax, directly after acknowledging that the adequacy of its data security measures were subject to the GLBA, FTC Act, and state data protection laws, among others, assured investors that it was compliant with those laws, stating, “We continuously monitor federal and state legislative and regulatory activities that involve credit reporting, data privacy and security to identify issues in order to *[remain in compliance] with all applicable laws and regulations.*”

60. Similarly, Equifax’s SEC filings touted the Company’s significant efforts to ensure it was compliant with data protection laws and regulations:

We are subject to a number of U.S. and state and foreign laws and regulations relating to consumer privacy, data and financial protection *We devote substantial compliance, legal and operational business resources to facilitate compliance with applicable regulations and requirements.*

61. In addition, Equifax issued statements on its website assuring the public, including investors, that Equifax’s data protection infrastructure complied

with cybersecurity industry best practices “at all times”: “We regularly review and update our security protocols to *ensure that they continue to meet or exceed established best practices at all times.*”

3. Defendants Assured Investors That Equifax Had Adequate Internal Controls

62. In the Company’s Class Period SEC filings, Defendants repeatedly represented and certified the adequacy of Equifax’s internal controls. These procedures and processes are designed to protect the Company’s assets and provide a means to ensure that Equifax’s public disclosures appropriately reflect the Company’s internal realities. Specifically, in Equifax’s Class Period Forms 10-K it disclosed that the Company had “effective” internal controls that would provide “reasonable assurance regarding *prevention or timely detection of unauthorized acquisition, use or disposition of our assets.*” Also, in connection with each of Equifax’s Class Period reports on Form 10-K and Form 10-Q filed with the SEC, Defendants Smith and Gamble signed certifications pursuant to the Sarbanes-Oxley Act (“SOX”), specifically certifying that these, and other controls would prevent the Company’s disclosures from being misstated.

63. However, Equifax lacked adequate internal mechanisms for protecting the Company’s data and detecting breaches of its data networks, and failed to design and implement an adequate data breach protocol that would facilitate prompt and complete disclosure of such breaches. Accordingly, Defendants’ statements concerning the Company’s internal controls were materially false and misleading.

D. In Truth, Equifax Failed to Adequately Secure and Protect Sensitive Consumer Information

64. In truth, and unbeknownst to investors, Equifax’s data security systems and cyberdefenses were woefully inadequate to protect the Company from intrusions and data theft, and failed to comply with applicable law and standard industry practices. As analysts, experts, and commentators have explained, the Data Breach publicly revealed the profound and systemic deficiencies in Equifax’s data protection infrastructure, which implicated both the Company’s technological and organizational commitment to cybersecurity. The widely-read cybersecurity publication Security Boulevard observed, for example, that

[s]ecurity is a discipline of layered defenses and controls that all contribute to the adequate prevention, detection, and response to a data breach. Nearly every company will fail, to some degree, at prevention. ***To have a breach of the magnitude Equifax has experienced one has to fail substantially at prevention, detection, and response.***

Indeed, Smith himself, in his testimony before the House Financial Services Committee, ***admitted*** that Equifax simply failed to “have preventative measures in place to combat a data breach of this magnitude.”

65. As discussed in greater detail below (including in Section H), Equifax’s undisclosed and misrepresented improper security practices included the following:

- ***Equifax failed to implement an adequate patch management process and failed to remediate known deficiencies in its cybersecurity infrastructure.*** As discussed below, Equifax relied on a single individual to manually implement the Company’s patching process across the entirety of its vast network. Because Equifax failed to properly inventory its “attack surface” (a fundamental security measure) – the number of components, systems and assets – the potential entry points for intruders — this individual had no way

of knowing where vulnerable software was being run and where patching needed to be implemented. Contrary to Defendants' statements that the Company implemented "advanced security, protections and redundancies," Equifax's patching process ran without adequate redundancies and oversight, and failed to adopt the automated patching processes that many peers implemented.

- ***Equifax failed to implement adequate encryption measures to protect sensitive information in its custody.*** As Equifax has admitted, sensitive personal information residing in its systems relating to hundreds of millions of Americans was not encrypted, but rather was stored and transmitted in plaintext, making it easy for intruders to read and misuse. Data that Equifax has admitted it failed to encrypt includes (1) sensitive data that was accessible through public-facing web portals, and (2) core credit file data. Moreover, even in cases where Equifax did encrypt sensitive data, it recklessly left the keys to unlock that encryption on its public facing networks.
- ***Equifax failed to implement adequate authentication measures.*** "Authentication measures" are mechanisms, such as passwords, used to verify that a party attempting to access a system or network is authorized to do so. As discussed below, Equifax relied on weak passwords and security questions to protect highly sensitive data. Among other things, Equifax continued to use four digit PINs based on Social Security numbers and birthdays to guard personal information, even after hackers repeatedly bypassed those "passwords," and even after Equifax explicitly agreed to stop using them. Likewise, Equifax "protected" a highly sensitive credit database with the username 'admin' and password 'admin.' Equifax also failed to implement standard authentication measures such as multi-factor authentication – a failure considered "a critical lapse in security practice."
- ***Equifax failed to adequately monitor, and establish mechanisms for monitoring, its networks and systems to detect compromises.*** As discussed below, and as a February 2018 report issued by Senator Warren ("Warren Report") concluded, Equifax failed to log and review network access, set up processes for tracking malicious scripts, or implement other standard practices used to monitor activity across systems and detect suspicious or dangerous behavior. Indeed, former Equifax employees reported that the Company

wholly failed to monitor changes in files and software – a basic cybersecurity requirement – “even on systems with sensitive information.”

- ***Equifax stored personal data so that it was easily accessible through public channels.*** As discussed below, Equifax stored and maintained sensitive personal information so that it was accessible (in unencrypted, plaintext form) through public-facing servers and web portals. Further, Equifax failed to employ standard “partitioning” of sensitive data – *i.e.*, isolating critical assets from one another across a network – so as to limit exposure in case of a breach. This is the digital analog of a bank leaving all of its most valuable assets in a single pile in its lobby.
- ***Equifax’s systems relied on outdated and obsolete software.*** Directly contrary to the Company’s statements during the Class Period, including that it deployed “advanced security, protections and redundancies” and “regularly review[s] and update[s] our security protocols,” Equifax relied on old and obsolete software, making its systems vulnerable to attack and exacerbating the harm caused by data breaches.
- ***Equifax failed to warehouse obsolete personal information.*** Equifax failed to safely dispose of sensitive personal information that was no longer needed or in use. Indeed, as alleged below, Smith told a handful of investors in private discussions after the Class Period that the Data Breach was so extensive partly because hackers had penetrated legacy databases containing decade-old information. Likewise, in Congressional testimony after the Class Period, interim CEO Barros admitted that Equifax was just beginning the process of “dispos[ing] of the data that [Equifax] no longer need[s].”
- ***Equifax failed to constrain sensitive information using standard “least privilege” protections.*** As the Warren Report concluded, Equifax failed to limit access to sensitive personal information to those employees whose job responsibilities required such access. Instead, Equifax employees (and even former employees) had open access to personal information indiscriminately.
- ***Equifax failed to set a “tone at the top” that promoted data security within the Company and failed to ensure that employees responsible for data security were adequately trained and qualified.*** As former Equifax employees have reported, despite the Company’s public statements to the contrary, data security was not a priority at Equifax and it failed to retain a

qualified information security team. Likewise, cybersecurity experts have noted that the security failures associated with the Data Breach evince “a very poor focus on information security at the highest levels of the company.”

- ***Equifax failed to perform adequate system reviews.*** Equifax failed to heed the calls of its cybersecurity consultants to perform comprehensive system reviews – a failure that allowed hackers to roam Equifax’s systems undetected for months. Moreover, Equifax’s vulnerability scanning process was grossly deficient: scans were performed infrequently, examined only portions of Equifax’s systems, relied on outdated technology, and lacked redundancies.
- ***Equifax failed to develop an adequate data breach plan.*** As Equifax’s response to the Data Breach made clear, and as Smith has admitted, the Company failed to develop and implement a comprehensive data breach plan. Among other things, and as the Warren Report explained, Equifax’s data incident response plan had not been updated in over three years, contrary to Defendants’ statements during the Class Period, including that Equifax “regularly review[s] and update[s] our security protocols.”

66. The scope and breadth of the deficiencies in Equifax’s cybersecurity demonstrate that the Company’s failures were not isolated or anomalous, they were pervasive and egregious. Equifax’s numerous wholly improper security practices evince a systemic and institutional disregard for cybersecurity at the Company’s highest levels, which made a significant data breach virtually inevitable. As *Wired* reported in a September 2017 article:

The accumulation of missteps, slow disclosure, and problematic public response with so many millions of innocent consumers potentially affected deeply troubles security practitioners. ***‘These are all indicators of a company that had a horrible security culture,’*** says Tinfoil Security’s [cofounder, Michael] Borohovski.

Likewise, the Institute for Critical Infrastructure Technology (“ICIT”), a leading cybersecurity think tank, found that “[a] catastrophic breach of Equifax’s systems

was inevitable because of *systemic organizational disregard for cybersecurity and cyber-hygiene best practices.*”

67. Moreover, Defendants were reminded again and again, both before and during the Class Period, that Equifax’s data protection measures were wholly inadequate. Indeed, many of Equifax’s less significant data security incidents leading up to the Data Breach resulted from a core group of similar, and very serious, weaknesses. Yet, astonishingly, Defendants failed to correct the glaring deficiencies and gaping holes in Equifax’s cyber-defenses, even as they touted the Company’s commitment to cybersecurity and compliance with data protection laws to investors.

E. Equifax Ignored Numerous Warnings That Its Data Protection Measures Were Inadequate to Protect Sensitive Information

68. By the start of the Class Period, it was clear to Defendants that the Company’s data protection regime was inadequate to protect the Company from significant intrusions. Evidence of the inadequacy of Equifax’s security posture continued to mount during the Class Period.

1. In 2013 and 2014 Equifax Experiences Breaches Due to Inadequate Cybersecurity

69. For example, prior to the start of the Class Period, Equifax had knowledge of numerous red flags concerning the inadequacy of its authentication measures (*e.g.*, password protection). In March 2013, Equifax acknowledged an intrusion into its system after information pertaining to celebrities and high-profile figures ended up on a website called Exposed. Sensitive data – including Social

Security numbers, credit reports, former addresses, and personal banking information – relating to former First Lady Michelle Obama, former Secretary of State Hillary Clinton and former Federal Bureau of Investigations (“FBI”) Director Robert Mueller, among others, ended up on the site after attackers gained “fraudulent and unauthorized access” to their credit reports. The hackers gained unauthorized access to data on Equifax’s computer systems by using publicly available information to answer security questions and bypass authentication measures.

70. Just one month after acknowledging this hack, Equifax experienced yet another intrusion arising from the Company’s failure to implement adequate authentication measures. Equifax admitted in a March 2014 letter to the New Hampshire Attorney General that beginning in April 2013, hackers penetrated Equifax and were “able to obtain [] credit reports using sufficient personal information to meet Equifax’s identity verification process,” just as hackers had done the year before. Because Equifax failed to implement adequate network monitoring safeguards, hackers were able to repeatedly penetrate Equifax’s network for approximately eight months before the Company finally detected the “suspicious inquiries” in January 2014. In its March 2014 letter, Equifax assured the New Hampshire Attorney General that the Company would implement “additional monitoring and blocking measures” to protect at-risk information.

2. KPMG Flags Equifax's Unsafe Encryption Practices

71. Also in 2014, Defendants were alerted to the fact that Equifax's encryption protocols were grossly inadequate to protect personal information maintained by the Company. Specifically, in 2014, Equifax retained KPMG to perform a security audit, which found, among other things, that Equifax left private "encryption keys" – the "passwords" used to unlock encrypted data – on the same public network servers on which the encrypted data were stored. This egregious lapse in cybersecurity is akin to leaving the key to one's house in the lock, allowing anyone who gained access to the server to also gain access to the encryption keys. Astonishingly, screen shots published by hackers after the Class Period,³ indicate that Equifax continued to leave private encryption keys on its network servers throughout the Class Period, even after KPMG provided Equifax management with its security audit.

3. Equifax's "Attack Surface" Becomes Too Large to Defend

72. By the start of the Class Period, another dangerous deficiency in Equifax's data security posture had metastasized. According to security researchers, Equifax had thousands of websites exposed on the internet, amounting to massive sprawl and evincing a loose control of infrastructure. As a result, Equifax's attack surface was too large to manage and adequately protect. An analysis by cybersecurity consulting firm OutsideIntel published after the Class Period shows

³ See Appendix, Figure 1.

that Equifax was managing more than 5,200 websites as of September 2017. In a Peerlyst article, security expert Claus Cramon Houmann characterized the list of Equifax websites uncovered by the OutsideIntel report as

a big list. No, it's a huge list of domains they are managing, no matter how you view it. Managing this list of domains, and the web servers behind [them] and the DNS entries and so on, that in itself would require a rather well structured security operations department and a CISO in charge.

And, an October 26, 2017 *Motherboard* article reported that Equifax's unwieldy "attack surface" was among the issues that a security researcher specifically raised with Equifax in December 2016.

4. The W2Express Breach

73. No later than early April 2016, just weeks after the start of the Class Period, Defendants received yet another warning that Equifax's authentication measures were inadequate to protect the sensitive information the Company maintained. At that time, Stanford University notified 600 current and former employees that thieves had accessed their W-2 data through Equifax's W2Express website, a service which offers downloadable W-2 forms for companies (the "W2Express Breach"). Not long thereafter, a string of other employers, including grocery giant Kroger and Northwestern University, notified their current and former employees that their W-2 data was similarly compromised. As noted cybersecurity expert Brian Krebs explained, hackers were able to access the W-2 data of hundreds of thousands of employees across numerous companies that had contracted with

Equifax to custody this information, “merely by entering at Equifax’s portal the employee’s default pin code, which was nothing more than the last four digits of the employee’s Social Security number and their four-digit birth year.” As discussed further below, the use of a four-digit pin code, let alone one based on personal identifiers (*e.g.*, a birthday or Social Security number), to provide authentication protection egregiously contravenes basic tenets of data security best practices. Yet, according to a Kroger spokesperson quoted by Krebs’ website *KrebsOnSecurity*, use of these flimsy default authenticators was “the standard Equifax setup.”

74. Once again, Equifax’s inadequate network monitoring practices compounded the magnitude of its failure to implement proper authentication protocols: the W2Express hackers first penetrated the Company’s networks in early 2015 and *remained undetected inside Equifax’s networks for approximately one year before they were discovered*, just as hackers had done during the cyberattack that occurred the previous year. As Forbes reported in a September 8, 2017 article, the W2Express Breach “resulted in the leak of 430,000 names, addresses, social security numbers, and other personal information” of consumers.

75. In the wake of the W2Express Breach, Equifax vowed to correct the issues causing it and issued a wave of soothing statements. First, as part of the settlement of a lawsuit brought by a Kroger employee arising from the breach, Equifax agreed to fix the glaring security issue that allowed the breach to occur and refrain from using “default PINs containing personally identifiable information to

access their W-2 information.” Notwithstanding this agreement, Equifax continued to use personal identifiers to set pin codes throughout the Class Period. Second, Equifax, including Defendants, issued statements falsely denying that the W2Express Breach implicated the Company’s security practices more broadly. For example, Smith reassured investors about the strength Equifax’s data protection measures at a May 2016 investor conference, shortly after *KrebsOnSecurity* first reported the W2Express Breach. Specifically, Smith stated that Equifax’s cyberdefenses were “in a very good position now,” and that to the extent there were any security lapses that contributed to the W2Express Breach, they were “within [the customers’] four walls. *It had nothing to do with us.*” This statement was not accurate because in truth, Equifax implemented inadequate authentication protocols to safeguard access to the information it maintained and stored on its networks.

5. Equifax Is Warned Repeatedly About Patching Deficiencies

76. Notwithstanding Defendants’ soothing statements, and unbeknownst to investors, Defendants continued to receive warnings that the Company’s data protection systems were inadequate as the Class Period progressed, but failed to fix the underlying problems. Among other things, Equifax was *specifically* notified that its patching processes were inadequate to protect sensitive information – a deficiency that figured prominently among the causes of the Data Breach.

77. Regarding those warnings, in an October 26, 2017 article entitled “Equifax Was Warned,” *Motherboard* reported that according to a former member

of Equifax's cybersecurity team who left the Company in 2017, the Company had hired Deloitte to perform a security audit in 2016. *Motherboard* reported that “[t]he audit found several problems, including a careless approach to patching systems, according to the former [cybersecurity] employee.” Equifax, however, failed to heed the report's warnings and address these deficiencies. The *Motherboard* article quoted the former cybersecurity team member as stating that when the cybersecurity team discussed the Deloitte report with the Company's management, “[n]obody took that security audit seriously.” This reality was borne out by the Data Breach.

78. Other former Equifax employees interviewed by *Motherboard* explained that, under Smith's stewardship, Equifax had long ignored the fact that its systems patching process was deficient:

One person, who worked at Equifax around 10 years ago, recalled that during his time there he warned the company of some servers that needed to be patched because they had open file-sharing ports that could be exploited by worms. The company did nothing, and, three months later, some servers got infected with the infamous Conficker worm, the source said. ***“It's [i.e., the Data Breach is] the same problem, but 10 years later,”*** the source said.

As discussed further below, Equifax and its executives, including Smith, continued to receive specific warnings about the inadequacy of the Company's patching process during the Class Period.

6. Throughout the Class Period Security Researchers Continue to Warn Equifax About Serious Cybersecurity Deficiencies, but These Warnings are Ignored

79. Throughout the Class Period, cybersecurity researchers privately alerted Equifax to numerous failures and deficiencies in its cyberdefenses. For example, on March 14, 2016, a security researcher notified Equifax that the Company’s main website was vulnerable to dangerous cross-site scripting attacks. Cross-site scripting vulnerabilities, also known as “XSS,” allow attackers to send specially-crafted links to Equifax customers and, if the target clicks through and is logged into the site, their username and password can be revealed to the hacker. As shown in the researcher’s September 7, 2017 Tweet reproduced in the Appendix,⁴ the researcher checked Equifax’s website and found that this vulnerability had *still* not been remediated, though it had been reported *a year and a half earlier*. In September 2017 *Forbes* quoted the researcher: “It really looks like they don’t care about security on their website – not surprised they got breached, certainly easily.”

80. Likewise, the October 2017 *Motherboard* article reported that a security researcher warned Equifax in December 2016 that an immense cache of personal consumer information was easily accessible through one of its public-facing websites in unencrypted form – the very issue implicated in the Data Breach. Specifically, *Motherboard* reported that the security researcher warned Equifax that one of its public-facing websites “displayed several search fields, and anyone – with

⁴ See Appendix, Figure 2 and Figure 2A.

no authentication whatsoever – could force the site to display [consumers’] personal data,” including social security numbers, full names, birthdates, and city and state of residence. The researcher explained that the “site looked like a portal made only for employees, but was completely exposed to anyone on the internet.” The researcher used a basic “forced browsing” bug – an exceedingly simple attack – to access reams of highly sensitive data; *Motherboard* reported that it “saw multiple sets of the data [the researcher] was able to access.” The researcher easily discovered this dangerous vulnerability “[i]n just a few hours, after scanning the company’s public-facing infrastructure.” The security researcher told *Motherboard*, “All you had to do was put in a search term and get millions of results, just instantly – in cleartext [i.e., unencrypted], through a web app.” The researcher further told *Motherboard* that “they downloaded the data of hundreds of thousands of Americans in order to show Equifax the vulnerabilities within its systems,” thus providing Equifax with undeniable evidence that sensitive data in its care was easily accessible through a public-facing website, was unencrypted, and was highly vulnerable to attack. The researcher told *Motherboard*, “***I’ve seen a lot of bad things, but not this bad.***”

81. Just as with the XSS vulnerability reported in March 2016, however, Equifax failed to remediate these deficiencies, and did not even take down the public facing site until June 2017 – six months after it had been reported – by which time Equifax’s systems had already been breached. The security researcher told *Motherboard*:

It should've been fixed the moment it was found. It would have taken them five minutes, they could've just taken the site down" I couldn't believe it, it was shocking," they told me. It was just disgusting to see them take this long to do anything about it.

82. The security researcher also told *Motherboard* that they reported additional serious cybersecurity deficiencies to Equifax in December 2016:

While probing Equifax servers and sites, the researcher said that they were also able to take control – or get shell access as hackers refer to it – on several Equifax servers, and found several others vulnerable to simple bugs such as SQL injection, a common, basic way of attacking sites.

SQL injections are highly dangerous vulnerabilities that allow attackers to easily trick the database portion of a website (which stores data) into running malicious commands.⁵ Fortunately, there are extremely simple defenses to this vulnerability, which are articulated in standard cybersecurity publications and resources.⁶ However, contrary to cybersecurity best practices, Equifax failed to implement these defenses, and its systems remained susceptible to these dangerous, but easy-to-fix, vulnerabilities throughout the Class Period, despite the fact that the Company was specifically warned about them.

83. Finally, *Motherboard* reported that the security researcher alerted Equifax in December 2016 that “[m]any [of the Company’s] servers were running

⁵ For example, suppose a website allows users to enter a username and check their records. A SQL injection allows a hacker to enter a username (*e.g.*, “Bob”) coupled with a malicious command (*e.g.*, “Bob and give me all users’ Social Security numbers”) to fool the website into believing the commands are legitimate.

⁶ *See, e.g.*, www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet.

outdated software.” However, as other security researchers later confirmed, Equifax continued to rely on old and outdated software to power its servers and websites throughout the Class Period, further increasing the Company’s vulnerability to attack. Indeed, cybersecurity experts later noted that Equifax’s reliance on obsolete and outdated software contributed significantly to the Data Breach.

7. The LifeLock Breach

84. No later than January 6, 2017, Equifax learned that another “technical issue” affecting its data systems compromised sensitive credit information belonging to consumers who purchased identity-theft protection services from Equifax partner, LifeLock. Equifax provides LifeLock members with credit information through an online portal. As a result of the “technical issue” affecting its data systems, Equifax allowed LifeLock customers to view credit information relating to *other customers*.

8. The TALX Breach

85. Less than a month later, by no later than February 1, 2017, Equifax discovered yet another data breach, this time in its Workforce Solutions business, resulting from the same deficiencies in the Company’s authentication and monitoring practices implicated in prior breaches, including Equifax’s use of weak passwords that relied on personal identifiers (the “TALX Breach”). This was the same improper security practice that was among the most salient causes of the W2Express Breach in 2016, as well as the 2014 and 2013 hacks described above.

86. Despite Equifax’s explicit agreement following the W2Express Breach to refrain from doing so, Equifax used personal identifiers and weak 4-digit PINs to

“protect” sensitive wage and W-2 data maintained by its TALX division, now called Equifax Workforce Solutions. From April 2016 to March 2017, hackers were able to exploit Equifax’s use of personal identifiers to reset the flimsy 4-digit PINs assigned to employees of Northrop Grumman Corp., Whole Foods Market Inc., Allegis Global Solutions Inc., and other Equifax clients whose data were stored in the division’s database. Hackers could then download the employees’ sensitive W-2 data, which could be used, among other things, to file fraudulent tax returns. As *KrebsOnSecurity* explained, “Equifax’s subsidiary TALX – now called Equifax Workforce Solutions – aided tax thieves by relying on outdated and insufficient consumer authentication methods.”

87. As with past hacks, Equifax’s poor network monitoring greatly amplified the damage done by the TALX Breach as intruders were able to freely access this sensitive data for *over a year* to file fraudulent tax returns and steal the refunds before they were finally detected. Equifax’s security and network monitoring was so poor that, as the Company admitted in a May 15, 2017 letter to the New Hampshire Attorney General, it could not even determine how many tax records were accessed without authorization.

88. The TALX Breach thus exploited a known vulnerability – one Equifax had explicitly agreed to fix – and resulted in the theft of data that Equifax knew was a high value target because it had been stolen in previous hacks, including a hack Equifax had discovered just one month before the TALX Breach began.

89. Security experts noted that the authentication protections Equifax had put in place to protect the W-2 data stolen in the TALX Breach were profoundly inadequate and failed to meet basic cybersecurity industry standards. For instance, cybersecurity expert Avivah Litan told *KrebsOnSecurity*, “Equifax should have known better than to rely on a simple PIN for a password That’s so 1990s It’s pretty unbelievable that a company like Equifax would only protect such sensitive data with just a PIN.” Instead, “Litan said TALX should have required customers to use stronger two-factor authentication options, such as one-time tokens sent to an email address or mobile device.”

90. Equifax once again issued a number of soothing statements about its cyberdefenses in the wake of the TALX Breach. In its letter to the New Hampshire Attorney General, Equifax said that “to help prevent recurrence of this type of incident, TALX has implemented additional security measures, including enhanced fraud monitoring and removal of personal questions as an option to reset PINs from the online portal,” though Equifax had already agreed one year earlier to refrain from using personal identifiers as part of its authentication process. Equifax further stated that it would implement two-factor authentication, as cybersecurity experts stated the Company should have done from the outset. Unbeknownst to investors, however, *Equifax continued to use personal identifiers to protect TALX data* (it used Social Security numbers as usernames and birthdays as passwords) even after the TALX Breach. Despite its representations to the New Hampshire Attorney

General and in its W2Express settlement stipulation, Equifax continued this practice until October 8, 2017, when *KrebsOnSecurity* first reported it. On October 8, 2017, Equifax finally took down the TALX site for “maintenance” and restored it thereafter with added layers of security.

9. Equifax Hires Mandiant, But Ignores Its Advice

91. Notwithstanding the Company’s reassuring public statements, Equifax internally recognized that its data security systems were rife with vulnerabilities. Accordingly, in the wake of the TALX Breach, Equifax hired cybersecurity firm Mandiant to investigate weaknesses in its data protection systems. Critically, *Smith was personally overseeing, and closely monitoring the progress of, this investigation*. As *Bloomberg* reported on September 29, 2017, despite Equifax’s reassuring statements downplaying the TALX Breach,

there are signs that Smith and others were aware something far more serious was going on. The investigation in March was described internally as ‘a top-secret project’ and *one that Smith was overseeing personally*, according to one person with direct knowledge of the matter.

92. Mandiant’s review quickly confirmed that Equifax’s data protection systems were grossly inadequate and specifically pointed to, among other things, the Company’s failure to patch vulnerabilities. *Bloomberg* reported, “Mandiant warned Equifax that its unpatched systems and misconfigured security policies could indicate major problems, a person familiar with the perspectives of both sides said.”

93. Equifax, however, failed to heed Mandiant's warnings, and instead, *Bloomberg* reported, after getting into a dispute with the consultant over its findings, "squelched a broader review of [Equifax's] security posture." Equifax's disagreement with Mandiant came just as the hackers who perpetrated the Data Breach were beginning to get a foothold into Equifax's network. The *Bloomberg* article stated that Equifax's failure to take Mandiant's findings seriously and perform an appropriately broad review of the Company's cybersecurity infrastructure "looks to have given the intruders [behind the Data Breach] room to operate freely within the company's network for months."

94. The inadequacy of Equifax's review of its cybersecurity posture is confirmed by internal Equifax emails, the contents of which were made public after the Class Period. In a January 26, 2018 article, the *New York Times* described an "urgent email and spreadsheet from inside Equifax" that the Company had inadvertently emailed to an individual outside Equifax. According to the article, the email "warned of 'inappropriate access' across several company systems and a 'lack of adequate review of operating system and database credentials.'" The article reported that the email asked recipients to "mark terminated employees in red, presumably so they wouldn't have access to internal systems anymore."

F. Equifax's Failure to Implement Basic Data Protection Measures Leads to The Massive Data Breach

95. On or about March 7, 2017, security firms began warning that attackers were actively exploiting a vulnerability in Apache Struts, an open-source software

application used to build interactive websites. Apache Struts is widely used by large businesses, including, by some estimates, 65% of the Fortune 100 companies. The software is ideal for websites where customers need to complete online forms. At Equifax, Apache Struts powered the website through which consumers can dispute errors in credit reports, and was a core part of the Company's web-based infrastructure.

96. On March 7, 2017, the security firms reported that Apache Struts was vulnerable to a "remote code execution" attack, a remarkably dangerous exploit. Remote code execution attacks make it possible for attackers to force vulnerable systems to run computer programs written by the attackers, which can make it simple to either steal data or gain a foothold within a vulnerable system. The vulnerability affecting Apache Struts was not only highly dangerous, it was particularly easy to exploit. Specifically, an attacker would simply need to send a malicious instruction to Equifax's dispute portal and would gain direct access to the underlying operating system – the digital equivalent of climbing through an unlocked window to sneak into a building. The vulnerability was, by any measure, critical.

97. Given the highly dangerous nature of the Apache Struts vulnerability and the software's widespread and extensive use in the business community, the exploit and the update developed to address it were widely publicized. On March 7, 2017, as soon as security firms began reporting on the vulnerability, Apache published its own notice of the vulnerability in its online security bulletins S2-045

and S2-046. Directed to “All Struts2 developers and users,” the Apache Security bulletins warned that the software was vulnerable to “Remote Code Execution,” which allows a hacker to send code to a website in order gain access to, and run commands on, the website’s server. The Apache bulletins ranked the vulnerability as “*critical*,” the “maximum security rating.” The vulnerability was also published in the Common Vulnerabilities and Exposure (“CVE”) database, a catalogue of known security threats sponsored by DHS, and assigned the CVE identifier CVE-2017-5638.

98. By March 8, 2017, Apache had released new versions of its software to mitigate the vulnerability. That same day, Cisco Systems, Inc. – a highly prominent global information technology company – also published a notice of the vulnerability and the accompanying “patch.” Cisco reported that it found “a high number” of examples where the hack had already been used.

99. Notably, on September 18, 2017, the *Wall Street Journal* reported that on March 8, a financial firm, justifiably concerned about the dangerousness of the Apache Struts exploit, specifically asked Equifax whether it had shored up any vulnerabilities with the new security patch. Equifax falsely reported that “it didn’t have an issue,” but did nothing to actually determine whether it did “have an issue.”

100. On March 9, 2017, Equifax received additional warnings that it needed to patch the dangerous Apache Struts vulnerability immediately. That day, DHS’ Computer Emergency Readiness Team (“U.S. CERT”) *sent Equifax an email*

individually notifying the Company of the vulnerability, which it characterized as “high” severity, and *specifically instructed Equifax to implement the published patch*. The next day, on March 10, the United States Department of Commerce’s National Institute of Standards and Technology (“NIST”) publicized the flaw in its National Vulnerability Database, *scoring the vulnerability’s severity at 10* on two different versions of the Common Vulnerability Scoring System. 10 is the highest possible score on either scale. NIST also noted that the Apache Struts vulnerability “allow[s] unauthorized disclosure of information” and would be low in complexity to accomplish. NIST provided over twenty other website resources for advisories solutions and tools relating to vulnerability and how to fix it.

101. Because Apache Struts is so widely used across the commercial sector, and because the exploit was exceedingly dangerous, computer and technology media outlets published numerous stories warning of the vulnerability and urging implementation of the patch. For instance, on March 9, 2017 alone, articles ran in prominent, widely-read publications with headlines that trumpeted the immense risk posed by the Apache Struts vulnerability, including: “Apache Struts 2 Needs Patching Now, Without Delay. It’s Under Attack Now. Black hats testing remote code execution zero-day vulnerability,” published in *The Register*; “Hackers Exploit Apache Struts Vulnerability to Compromise Corporate Web Servers,” published in *PC World*; and “Critical vulnerability under ‘massive’ attack imperils high-impact sites,” published in *Ars Technica*. *Ars Technica* further warned of a “string of attacks

that have escalated over the past 48 hours [where] hackers are actively exploiting a critical vulnerability that allows them to take almost complete control of Web servers used by banks, government agencies, and large Internet companies.” These stories about attempts to batter sites that had yet to apply the patch were available to Equifax and its executives, including Defendants.

102. Despite the fact that the Company received warning after warning to patch the Apache Struts vulnerability, including individualized and specific admonitions from DHS to do so, and despite the fact that the vulnerability itself was exceptionally dangerous and its exploitation would expose the most sensitive and valuable information maintained by Equifax to theft and abuse, and despite the fact that Apache Struts was a core part of Equifax’s web-based infrastructure, ***Equifax has admitted that it failed to install the patch it had been sent in notice after notice about the vulnerability.*** The vulnerability remained undiscovered and unpatched until July 30, 2017, when Equifax finally took down the affected web portal.

103. Smith’s own account of Equifax’s failure to remediate the Apache Struts vulnerability by installing a simple update demonstrates that the Company’s data protection processes and protocols were profoundly and fundamentally flawed during the Class Period. In Congressional hearings after the Class Period, Smith testified that ***one person*** in the Equifax was responsible for manually notifying the entire Equifax Information Technology (“IT”) team about this critical vulnerability and instructing them to patch it. According to Smith, Equifax’s immense cache of

highly sensitive consumer data was left vulnerable to exploitation and theft because of this single individual's failure. Smith testified at an October 4, 2017 hearing before the Senate Judiciary Subcommittee on Privacy, Technology and the Law that "the individual who was responsible for communicating to the organization to apply the patch did not." Smith also admitted in testimony before the Senate Judiciary Committee that not only was a single individual responsible for implementing a manual process to patch Equifax's vast networks, that *single individual did not even know (and apparently had no way to tell) what software Equifax had deployed through those networks* (and thus if and where patching should have been applied). Smith testified, "I am not certain that the individual who was responsible for communicating that the patch needed to be applied – that he knew the software was deployed." Smith's testimony is an admission that Equifax failed to maintain an inventory of its security assets, contrary to basic data protection practices.

104. Smith further testified that a scan of Equifax's network for vulnerabilities had been run on March 15, 2017, but failed to detect the Apache Struts vulnerability. This failure is entirely unsurprising, however, because as Smith's testimony made clear, the Company's vulnerability scanning was infrequent, relied on outdated technology, and lacked appropriate redundancies. Smith conceded in his testimony before the House that "You have got to tell [the scanner Equifax deployed] what it is looking for." Because Equifax's data protection processes depended on a single individual to provide manual notification

of vulnerabilities to the remaining IT team (which person failed to do so in this case), it made little sense for Equifax to have expected the IT team to program the scanner look for vulnerabilities about which it was never notified. Smith conceded that Equifax's systems were scanned for vulnerabilities only once during the time the Company received the March 8 email from CERT and the end of the Class Period. Additionally, in correspondence sent to Senator Warren, Equifax admitted that it – inexplicably – runs vulnerability scans on only part of its systems, and, in this case, failed to scan the vulnerable component of its network running Apache Struts.

105. In his testimony, Smith conceded that the scanner Equifax used during the Class Period was old and outdated. Smith told the Senate Commerce Committee, “What we had installed shortly after – about the time of the – on the last hearings, was a new scanning technology. We upgraded a scanning technology to a new-generation scanner that [] seems to be a better scanner than the prior scanner.” Smith's testimony is consistent with the findings of Macquarie securities analysts, who reported on September 15, 2017 that their testing and analysis indicated that industry standard scanners could detect the Apache Struts flaw without difficulty.

106. Outraged cybersecurity experts explained that Equifax's patching process as described by Smith was utterly deficient, failing to come close to a “reasonable standard of care.” An October 30, 2017 article in the prominent data security publication Security Boulevard, quoted cybersecurity expert Amit Yoran:

Former Equifax CEO Richard Smith's statement before Congress about the catastrophic breach affecting 145 million Americans *was*

dumbfounding. The company’s willingness to blame the breach on a single engineer not acting quickly enough to patch a known vulnerability can only be characterized as a total face-palm moment. In fact, the whole Equifax explanation is such a long series of face-palm moments that I now have a migraine. And ***how do you implement processes where the entire cyber infrastructure of Equifax and securing access to all of this incredibly sensitive information about hundreds of millions of people boil down to one person? In what world does this seem like a reasonable standard of care??***

107. Likewise, cybersecurity expert and columnist George Hulme wrote in an October 17, 2017 article entitled “No Mr. Equifax CEO You Don’t Get To Blame One ‘IT Guy’ For Your Breach,” also featured on *Security Boulevard*:

It’s inconceivable that the CEO of any company – especially any company whose primary value rests with being a good steward of data – [would] blame the breach on bad assessments and communication. Equifax aggregates information on more than 800 million consumers and 88 million businesses. Equifax has one commodity it trades: information and context on that information and consumers it reports upon. That’s it.

* * *

Security is a discipline of layered defenses and controls that all contribute to the adequate prevention, detection, and response to a data breach. Nearly every company will fail, to some degree, at prevention. To have a breach of the magnitude Equifax has experienced one has to fail substantially at prevention, detection, and response. A number of bad assessments and one IT person’s error is ***not an acceptable reason to fail at data breach prevention, detection, and response — not a company that is actually trying to secure its assets with adequate security personnel, processes, and tools. And it’s not a reason the world will accept, either.***

108. At an October 5, 2017 House Financial Services Committee hearing, Representative Carolyn Maloney pointed out that, in contrast to Equifax's inadequate manual patching process, Equifax's peers deployed a fully automated process that successfully detected the Apache Struts vulnerability. Experian, she said, has a patch management system that

will literally shut down [the vulnerable system] – it won't even work, it shuts down automatically – if a patch isn't implemented immediately. So my question is, why didn't your patch management system automatically shut down your systems when the security patch wasn't implemented? Why was this flaw allowed to go unpatched for months before you noticed it?

109. In mid-March 2017, following Equifax's failure to install the Apache Struts patch, hackers scanning the internet for computer systems vulnerable to the attack got a hit on an Equifax server in Atlanta. According to a confidential note obtained by the *Wall Street Journal*, after interacting with Equifax's server, the hackers entered the computer command "Whoami." This command would have given the attackers the username of the computer account to which they had just gained access, an early step in a hacking attempt. Before long, the hackers easily exploited the gaping hole the Company's poor security had left in its networks.

110. According to an internal Equifax analysis obtained by *Bloomberg*, the hackers that first breached Equifax's network via the Apache Struts vulnerability, known as the "entry crew," were a reconnaissance team searching for further vulnerabilities and testing systems to determine whether they stored anything of

value. However, Equifax's inadequate network monitoring and patching processes, coupled with its failure to perform the comprehensive security review Mandiant had urged the Company to undertake, gave attackers valuable time to analyze Equifax's systems and pass the attack off to a more sophisticated team of hackers.

111. Equifax's post-breach internal analysis, as described by *Bloomberg*, makes clear that because Equifax failed to adequately review the Company's data protection systems and monitor its networks, these hackers gained critical time to "customize their tools to more efficiently exploit Equifax's software, and to query and analyze dozens of databases to decide which held the most valuable data."

112. According to the *Wall Street Journal*, an internal Equifax report stated that on or about May 13, 2017, the hackers accessed files containing Equifax usernames and passwords, which they used to access "documents and sensitive information stored in databases in an Equifax legacy environment." This legacy environment stored old data that Equifax no longer used, but, unaccountably, still maintained on vulnerable public-facing networks. The *Wall Street Journal* further reported that in private meetings with select investors after the Class Period, Smith and Gamble stated that legacy databases that were hacked "retained consumer information going back five to 10 years," which "was part of the reason so many people were affected."

113. The internal Equifax report also stated that the attackers accessed "numerous database tables in several databases," and "compromised two systems"

that support Equifax's online dispute web application. Indeed, the hackers had so much time to roam around Equifax's internal systems undetected, they eventually set up about 30 Web shells – hidden pages that would allow them to remotely run commands on Equifax's systems even if the Struts vulnerability was patched.

114. Ultimately, the trove of immensely valuable personal consumer information the hackers collected was so large it had to be broken up into smaller pieces to try to avoid tripping alarms as data slipped from Equifax's grasp through the summer. Again, because of Equifax's failure to adequately monitor its systems, implement a patching process meeting basic industry standards, or perform a reasonable review of its systems as urged by its security consultants, the hackers had more than enough time to break up the data and exfiltrate it from Equifax.

115. The hackers took names, Social Security numbers, birthdays, addresses, driver license information (including driver license numbers, issue dates, and states), tax identification numbers, and other personal data belonging to 148 million Americans, as well as credit card information for 209,000 consumers. The hackers also took personal information belonging to nearly 1 million foreign consumers and employees, including Canadian and British citizens. As discussed below, the fact that Equifax allowed highly sensitive personal information to be accessible through a public-facing web portal, rather than appropriately partition the sensitive data, was yet another astonishing security failure. Shockingly, not only were these data left

out in the open, they were *not encrypted* on Equifax's systems; instead, they were stored in simple plaintext, making it easy for the hackers to read.

116. On July 29 and 30, 2017 – a Saturday and Sunday – Equifax finally discovered the hackers. As the Company acknowledged in its post-Class Period statements, discussed below, it was immediately clear to Equifax that hackers had gained “unauthorized access” and “criminal access” to its network.

117. On July 31, 2017, Chief Security Officer (“CSO”) Susan Mauldin, who had already been alerted of the Data Breach, contacted Chief Legal Officer John Kelly – on a Sunday – to notify him about the breach. At an October 3, 2017 House Committee on Energy and Commerce hearing, Representative Jan Schakowsky discussed the substance of an interview with Mauldin conducted by her staff. According to Representative Schakowsky, Mauldin stated that she told Kelly during “the week of July 30th that the Data Breach ‘might have compromised personally identifiable information.’” The *Wall Street Journal* reported that Mauldin told Representative Schakowsky's staffers that “she shared the possibility of personal information being compromised because of results from a sampling of data that Equifax had done in the wake of the July 29 discovery.”

118. Smith was notified of the Data Breach on Monday July 31, 2017, the first business day after Equifax has claimed the breach was discovered. That day, Kelly emailed Smith to tell him that CIO Webb would meet with him personally to discuss a data security issue. Importantly, as *Bloomberg* reported, Equifax's

“[p]rotocol included alerting the chief of security, who determined the severity of the breach, and then telling the executive leadership if a threat was considered serious.” In other words, the fact that Smith was notified demonstrates that Equifax executives considered the Data Breach to be “serious” no later than July 31, 2017.

119. At a hearing of the House Committee on Energy and Commerce, Smith testified that his July 31, 2017 meeting with Webb was “the first time [he] heard about the breach of security.” Smith further testified that Webb told him “that security had noticed a suspicious movement of data out of [*i.e.* an exfiltration of data] an environment we call a dispute portal.” In response to Representative Gregg Harper’s question about whether Smith asked “if there had been any personal identifying information” involved in the attack, Smith acknowledged that “at the time I was informed it was a dispute portal document,” which as discussed above almost certainly includes personal information.

120. On August 2, 2017, Equifax notified the Federal Bureau of Investigation that hackers had gained “criminal access” to the Company’s network. Also on August 2, the Company asked King & Spalding LLP to “guide the investigation” into the Data Breach, and, that same day, the law firm retained Mandiant to assist with the investigation. Cybersecurity experts have noted that the dramatic steps the Company took in the days following its discovery of the Data Breach demonstrates that Equifax and its executives knew the attack was unusually

serious. For instance, in a September 8, 2017 article published on Savage Security, information security expert Adrian Sanabria explained:

I spent over five years of my career as the chief incident handler for some large organizations. I can tell you that my incident response plans would involve my CFO (along with the rest of the executive tier) knowing about something the size of this breach within a few hours of me finding out. In [a] video [statement released on September 7, 2017], Rick Smith says that the attacker's connection to their systems was *immediately* severed. That suggests the nature of the breach was quickly apparent. Furthermore, Smith says law enforcement was immediately notified and that a "leading cybersecurity firm" was engaged to conduct a "comprehensive forensic review." The latter action equates to lots and lots of expense[, indicating the CFO is likely to be notified].

(emphasis in original).

121. As discussed further below, in the days immediately following Equifax's purported discovery of the Data Breach and just after Smith was notified, Defendants Gamble and Ploder sold more than \$1 million in Equifax stock, part of a larger pattern of insider sales during the Class Period. On August 1, CFO Gamble sold \$946,374 worth of Equifax stock – more than 13% of his holdings. On August 2, Ploder sold 4% of his holdings, netting \$250,458. These sales were not prescheduled pursuant to a Rule 10(b)5-1 trading plan. Notably, Smith testified at an October 5, 2017 House Financial Services Committee hearing that Ploder and Gamble "would [have been] involved in many of the meetings" the CEO had about the breach. While it took Equifax 40 days to disclose the Data Breach, it took the Company's executives only three days to offload more \$1 million in stock.

122. According to Equifax, by no later than August 11, 2017, Mandiant confirmed that “in addition to dispute documents from online web portal, hackers may have accessed a database table containing a large amount of consumers’ NPPI, and potentially other data tables.” Again, Mandiant’s report echoed the conclusion that Mauldin had already shared with Kelly the previous week. At the same October 3 Congressional hearing, Smith testified that despite knowing about the Data Breach since July 31, 2017, he *first requested a briefing about it on August 15, 2017 – over two weeks later*. At that briefing, Smith testified that he “was informed that it appeared likely that consumer NPPI had been stolen.”

123. Astonishingly, at an August 16, 2017 Equifax investor conference, Defendants made statements touting the Company’s cybersecurity, despite knowing that large amounts of consumer information had been compromised as a consequence of the still-undisclosed Data Breach. Defendants stated, among other things, that Equifax’s “role as a Trusted Steward is a Key Execution Enabler” and assured investors that the Company was making “[c]ontinued investments to address critical data security throughout the company,” but failed to disclose that the Company’s abysmal security infrastructure had just been seriously compromised.

G. The Truth About Equifax’s Inadequate Cybersecurity Is Finally Revealed to Investors

124. The truth concerning Defendants’ fraud began to emerge on September 7, 2017 when Equifax belatedly disclosed the Data Breach, revealing the serious undisclosed weaknesses in the Company’s cybersecurity and laying bare its failure

to abide by the representations made to investors described in this Complaint. Defendants' disclosure came *six* months after hackers penetrated the Company and nearly a month and a half after Equifax personnel, including Smith, purportedly learned of the Data Breach. Subsequent disclosures occurring over the following days, ending on September 15, 2017, provided additional revelations concerning the details and impact of Defendants' fraud.

1. Revelations Affecting Trading on September 8, 2017

125. After the close of trading on Thursday, September 7, 2017, Equifax issued a press release disclosing that it had suffered a data breach affecting PI of approximately 143 American consumers. Specifically, Equifax's press release stated that "criminals exploited a U.S. website application vulnerability to gain access to certain files" sometime between May and July 2017. The compromised database contained NPPI (non-public personal information)—confidential customer information including names, Social Security numbers, birth dates, addresses, and driver's license numbers. Additionally, the Company said, the hackers accessed "credit card numbers for approximately 209,000 U.S. consumers, and certain dispute documents with personal identifying information for approximately 182,000 U.S. consumers[.]"

126. Equifax further stated that the Company:

[D]iscovered the unauthorized access on July 29, 2017 and acted immediately to stop the intrusion. The company promptly engaged a leading, independent cybersecurity firm that has been conducting a comprehensive forensic review to determine the scope of the intrusion,

including the specific data impacted. Equifax also reported the criminal access to law enforcement and continues to work with authorities. While the company's investigation is substantially complete, it remains ongoing and is expected to be completed in the coming weeks.

Equifax provided no further detail concerning its internal "investigation," when this investigation began, what it uncovered, or why Defendants were only now disclosing a May breach.

127. In the September 7 press release, Defendant Smith said:

This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do. I apologize to consumers and our business customers for the concern and frustration this causes[.] We pride ourselves on being a leader in managing and protecting data, and we are conducting a thorough review of our overall security operations. We also are focused on consumer protection and have developed a comprehensive portfolio of services to support all U.S. consumers, regardless of whether they were impacted by this incident.

128. Analysts reacted immediately to Equifax's disclosure of the Data Breach, with Cowen analysts describing the hack on the evening of September 7 as "one of the biggest cyber-attacks in US history" and noting that in light of the volume of "sensitive consumer data" stolen in the hack and Equifax's "cherished position with respect to consumer data," its stock would come under significant near-term pressure. J.P. Morgan similarly reported that evening that "[g]iven the proliferation of data breaches in recent years, we sense a general numbing by the public to such events, yet the scale of this breach – coupled with the fact that Equifax is a data company – will deservedly drive a large initial decline in the EFX share price."

129. Analysts also commented on the financial impact of the breach, with Stifel reporting on September 8 that the hack “is likely to cost the company materially, and costs could drag on for a number of years.” Target and Home Depot cases imply potential for \$300M-\$325M in costs, irrespective of near-term impact on revenue.” On the point of lost revenue, Evercore ISI also noted on September 8 that “[m]anagement is not quantifying the potential financial impact of this breach,” but that “[o]ver the next year . . . Equifax will be providing free Trusted ID Premier data breach services to consumers who choose to use them.” Thus, Equifax would be providing *free* services to up to 143 million US consumers to whom it typically seeks to sell such services. The same day, Stifel removed Equifax from its “Select List” of high-conviction stocks, citing “the opaqueness of the situation,” acknowledging that the Company had not yet provided much clarity regarding the Data Breach.

130. Before the opening of trading on September 8, 2017, the *Wall Street Journal* published an article quoting credit specialist and former Equifax manager John Ulzheimer as stating that “[t]his is the nightmare scenario – all four pieces of information in one place[.]”

131. Cybersecurity experts also immediately began reporting on Equifax’s egregious failures. After the close of trading on September 7, 2017 Gartner security analyst Avivah Litan told *Reuters* that “on a scale of one to 10, this is a 10 in terms of potential identity theft. Credit bureaus keep so much data about us that affects

almost everything we do.” On September 8, *Forbes* quoted a cyber security engineer as stating that “Equifax shouldn’t have allowed so much information to be accessible via a breach of its public-facing web applications. It definitely should not be possible to do what happened if security was sound.” Cyber security expert Brian Krebs also wrote in *KrebsOnSecurity* on September 8 that he could not

recall a previous data breach in which the breached company’s public outreach and response has been so haphazard and ill-conceived as the one coming right now from . . . Equifax, which rather clumsily announced Thursday that an intrusion jeopardized Social security numbers and other information on 143 million Americans.

132. Also on September 8, the FBI, and New York, Massachusetts, and Illinois attorneys general all announced that they were pursuing investigations concerning the Equifax Data Breach. Similarly, the House Financial Services Committee and the House Energy and Commerce Committee announced that they would hold hearings on the Data Breach. Also, during trading on September 8, 2017, Senator Warren tweeted that it was “outrageous that [Equifax] waited so long to disclose the breach – needlessly leaving nearly half of America at risk for a month.”

133. Equifax’s September 7 press release also identified a website – www.equifaxsecurity2017.com – “to help consumers determine if their information has been potentially impacted and to sign up for credit file monitoring and identity theft protection” through Equifax’s TrustedID Premier product (“TrustedID”) to customers who opted in. Equifax also encouraged consumers to “contact a dedicated call center . . . which the company set up to assist consumers.”

134. In addition to the revelation of the Data Breach itself, Equifax's haphazard response began to reveal to investors the woeful state of the Company's data security – and, among other things, that the Company lacked an adequate data breach response plan. For instance, consumers were unable to contact Equifax to determine whether their personal information had been compromised. As *Newsweek* reported before trading opened on September 8, 2017, upon contacting Equifax's "call center," customers were told, "at this time, we do not have a database of impacted individuals. I am unable to tell you whether you are impacted. We are a company that was hired by Equifax to provide call center services but as of this point they haven't provided us with that database."

135. Equifax instructed consumers to visit a website, described above, set up in response to the Data Breach, where they were prompted to enter certain identifying information to determine whether their data was compromised, including the last six digits of their social security numbers ("Data Breach Website"). Despite the fact that Equifax had known about the Data Breach for *weeks* before disclosing it, this website was poorly constructed and, in fact, was wholly insecure – a shocking cybersecurity failure in the wake of the Data Breach.

136. Among other things, Equifax set up the Data Breach Website on a "stock installation," or cookie-cutter version, of WordPress. This type of content management system does not provide the level of security required for a website prompting users to enter *six out of nine* of the digits of their social security numbers.

Astonishingly, Equifax's Data Breach Website used *expired security certificates*. Cyber security experts noted, the domain name for the Data Breach Website was not registered to Equifax and looked much like a phishing site. Moreover, a username for administering the Data Breach Website was accessible on the website itself. And, when the Data Breach Website was initially rolled out following the Company's Data Breach Disclosure, it was only intermittently available – a clear sign that Equifax had not developed a response for a large-scale data breach.

137. A September 8, 2017 *Ars Technica* article by Dan Goodwin said with regard to Equifax's response that:

It was bad enough that Equifax operated a website that criminals could exploit to leak so much sensitive data. That, combined with the sheer volume and sensitivity of the data spilled, was enough to make this among the worst data breaches ever. ***The haphazard response all but guarantees it.***

138. In response to Equifax's disclosure of the Data Breach and the revelations described reflecting the undisclosed problems with the Company's cybersecurity, shares of Equifax common stock plummeted. By market open on Friday, September 8, 2017, Equifax shares were down nearly \$21.00, and dropped by nearly 15% during the trading day, closing at \$123.23 per share, on extraordinarily high trading volume of 16.85 million shares.

139. Still, Defendants made every effort to quell fears regarding the upheaval caused by the Data Breach, with Equifax announcing on September 8 that

Defendants Smith and Gamble would meet with investors in New York on Tuesday, September 12, and in Boston on Wednesday, September 13.

140. In the days that followed Equifax's initial disclosure of the Data Breach, new information was revealed that continue to inform the market not only of the gravity of the breach, but of the fundamental defects in the Company's data security framework that enabled the breach to occur in the first place and to go undetected for so long, and of how significant the steps to remediation would really be.

2. Revelations Affecting Trading on September 11, 2017

141. More information reflecting Equifax's poor cybersecurity and planning was revealed after trading closed on September 8, 2017. For example, during the evening of September 8, 2017, Tom Hegel, Senior Threat Researcher at security firm ProtectWise, stated in response to Equifax's September 7 apology that "[t]he grim truth is your personal information is probably already in someone else's hands."

142. On Friday evening, September 8, 2017 the *Wall Street Journal* reported that the FTC had published a page advising consumers on how to protect themselves after the Data Breach and noting that at least one of the FTC's Commissioners was "very concerned about the sensitivity of the information and magnitude of the breach," further indicating that the FTC would investigate the Data Breach.

143. Regarding the Company's response to the Data Breach, on Sunday, September 10, 2017 the *New York Times* reported that the Data Breach Website

allowed consumers to elect to freeze their Equifax credit file and issued those consumers PINs that could be used to reverse the freeze. However, the PINs issued to consumers were simply *the date and time* the consumer signed up for the credit freeze. Accordingly, these “PINs” could be easily guessed and used by hackers.

144. Recognizing the problematic nature of addressing the Data Breach, and not being in a position to respond to investor or public inquiries, during the morning of Monday, September 11, Equifax canceled Defendant Gamble’s appearance at the Barclay’s Global Financial Services conference in New York. Later, in a post on its website listing “Investor Relations Q&A” about the Data Breach, Equifax stated: “Investors are an important constituency and we intend to continue a high level of accessibility and participation in conferences, NDR’s and other meeting requests.”

145. September 11, 2017 also brought news that government agencies, legislators, and state attorneys general were initiating investigations into Equifax, communicating to investors that, contrary to Defendants’ statements during the Class Period, Equifax wholly failed to comply with applicable data protection laws and regulations.

146. Specifically, during the trading day on Monday, September 11, 2017, Senators Orrin G. Hatch (R-Utah), Chair of the Senate Finance Committee, and Ron Wyden (Ore.), ranking Democrat of the Senate Finance Committee, announced their own probe of Equifax, and sent the Company what the *Washington Post* called a

“sternly worded letter” demanding not only answers about the Data Breach, but about Equifax’s data security efforts generally.

147. The letter from Senators Hatch and Wyden stated that the “scope and scale of this breach appears to make it one of the largest on record, and the sensitivity of the information compromised may make it the most costly to taxpayers and consumers[.]” The letter also “raised the prospect of ‘irreparable harm’” to critical government programs such as Social Security, Medicare, and Medicaid, “by helping criminals use false identities to seek government benefits and tax refunds.”

148. Senators Hatch and Wyden lodged detailed questioned concerning Equifax’s cybersecurity, demanding that Equifax explain the size and reporting structure of its security team, whether the Company worked to fix any previously identified vulnerabilities, and whether the company has an established system for receiving and evaluating reports about systemic vulnerabilities. The Senators also demanded answers to detailed questions about Equifax’s operations and how the Company dealt with past security breaches. The questions revealed the degree of alarm and concern regarding the underlying reasons for the Data Breach.

149. During trading on September 11, *Security Boulevard* published the results of a BitSight report on Equifax’s security capabilities, providing initial insight into the answers to the Senators’ questions about the Company’s data security. According to the Bitsight report, Equifax was rated an F in Application Security and a D in software patching. Security Boulevard noted that “with its F

rating for the past 60 days, Equifax was rated in the bottom 10 percent of all companies,” and further that “the Patching Cadence [*i.e.* software patching] history for Equifax [] steadily trended worse during the past year.”

150. Also on September 11, 2017, Standard & Poor’s revised its rating outlook for Equifax from “neutral” to “negative” in light of the Data Breach. An S&P Research Update published that day stated:

The negative outlook reflects substantial uncertainty surrounding the eventual impact of this incident. [W]ith considerable uncertainty, including potential for impacts on strategy, substantial litigation, fines and costs related to the incident, we expect that leverage could remain elevated above 2x over the next two years.

151. In response to the news released after the close of the markets on Friday, September 8, and through the trading day on Monday, September 11, including the serious issues with Equifax’s response to the Data Breach and the concerns raised about its cybersecurity reflected in the congressional probe, Equifax stock price fell again, closing at \$113.12 per share, down more than \$10 per share from its September 8 closing price – a further drop of 9% – on elevated volume of 9.83 million shares traded.

152. Barclays reported on Tuesday, September 12 that a “hack or breach is one of the worst things that can happen to any ‘data’ company, let alone a ‘consumer’ credit bureau,” and that “many view the stock as ‘un-investable’ with plenty of Q’s still to be answered.” The same report stated that “overhang” from the Data Breach would “weigh on the shares for at least the next 6-12 months” due in large part to

the “stream of negative news hurting the brand; lawsuits, hearings, investigations, and regulations[.]” The report also questioned why Equifax – a Company charged primarily with data security – could suffer such a significant data breach, asking “why [] this website [was] holding records on 143M consumers” and stating that Equifax, as a “data company should have been much better prepared to catch the breach early vs. 2.5 months later[.]”

153. In the face of this widespread scrutiny Equifax tried to reassure the market, tweeting on September 11 that the Company is “committed to updating consumers on steps taken to provide the support needed and address issues they face around this incident.” This attempt proved unsuccessful, as the *New York Post* reported that day that “[w]hile it’s too soon to tell whether the moves will placate irate consumers, it is clear investors are still looking to beat up the company’s stock.”

3. Revelations Affecting Trading on September 13, 2017

154. After the markets closed on September 12, 2017, *USA Today* published an editorial from Defendant Smith. In response to the numerous issues consumers were having with the Data Breach Website, Defendant Smith stated: “Consumers and media have raised legitimate concerns about the services we offered and the operations of our call center and website. We accept the criticism and are working to address a range of issues.” He added that “[t]his is the most humbling moment in our 118-year history.”

155. Beyond the apology, Smith finally gave the market hard numbers enabling investors to quantify for the first time since the Company disclosed the Data Breach the financial impact the breach was having – and would continue to have – on the Company. Regarding the number of U.S. consumers that had, to-date, taken advantage of the Company’s offer of complimentary TrustedID, Smith stated that “[a]s of Tuesday, more than 15 million people have visited the website and 11.5 million are enrolling in credit file monitoring and identity theft protection.” He reminded consumers that the Company “took the unprecedented step of offering credit file monitoring and identity theft protection to every U.S. consumer. Every consumer, whether affected or not, has the option of signing up for the services.”

156. Smith sought to allay the market’s concern about long delay in alerting the public to the Data Breach, recognizing that “many people are questioning why it took six weeks to report the incident to the public.” Smith stated that Equifax engaged “a leading cybersecurity firm to conduct an investigation” upon learning of the breach, and that “[a]t the time, we thought the intrusion was limited.” Smith added that Equifax was

devoting extraordinary resources to make sure this kind of incident doesn’t happen again. We will make changes and continue to strengthen our defenses against cybercrimes. We will make sure every consumer who wants protection has a full package of services. And we will continue to update everyone on our progress.

157. After the close of trading on September 12, 2017 and during the trading day on September 13, 2017, additional details about Equifax’s pervasive failure to

implement adequate authentication measures were revealed. U.S. cyber security firm Hold Security LLC had provided an analysis conducted on Equifax's South American operations after the Company disclosed the Data Breach in North America. The Hold Security report provided that "an online portal designed to let Equifax employees in Argentina manage credit report disputes from consumers in that country was wide open, protected by perhaps the most easy-to-guess password combination ever: '*admin/admin.*'"

158. The Hold Security report went on:

From the main page of the Equifax.com.ar employee portal was a listing of some 715 pages worth of complaints and disputes filed by Argentinians who had at one point over the past decade contacted Equifax via fax, phone or email to dispute issues with their credit reports. The site also lists each person's DNI – the Argentinian equivalent of the Social Security number – again, in plain text. All told, this section of the employee portal included more than 14,000 such records.

159. On September 13, 2017, during the trading day, Professor Alan Woodward, a UK-based cyber security expert, told the British Broadcasting Corporation (BBC) that

[t]his kind of security vulnerability is extraordinary as even the most basic of checks should reveal this[.] ***It's outrageous that any organization that holds such sensitive personal data can build a portal with this kind of basic security vulnerability.*** It simply shouldn't happen and responding that they have now fixed the issue is not the point: it puts a huge question mark over whether Equifax have [sic] been applying the appropriate resources to online security elsewhere.

160. On Wednesday, September 13, 2017, in response to this news concerning the “admin/admin” issue in Argentina, Equifax provided a brief, opaque statement:

We immediately acted to remediate the situation, which affected a limited amount of public information strictly related to consumers who contacted our customer service center and the employees who managed those interactions. We have no evidence at this time that any consumers, customers, or information in our commercial and credit databases were negatively affected, and we will continue to test and improve all security measures in the region.

161. CNET responded to this disclosure by stating that hackers “would have been able to read some 14,000 credit dispute complaints from ordinary Argentinian citizens, which were stored in plain text instead of being encrypted.”

162. As the severe failures in Equifax’s cybersecurity framework grew apparent and the market began to understand the unprecedented circumstances of the Data Breach, the *Wall Street Journal* reported on September 13, 2017, that “banks and other financial companies are considering the possibility of moving some business away from Equifax Inc. in the wake of its data breach and to some of the firm’s credit-reporting rivals[.]” The article further stated that “large banks . . . have expressed dismay privately that their customers’ information was compromised, that they received no advance warning of the breach announcement, and that they still have little insight into what went wrong[.]”

163. Also during the trading day on September 13, Reuters reported that a coalition of 40 states, led by Illinois Attorney General Lisa Madigan, joined together

in a probe of Equifax's handling of the Data Breach, further communicating to investors that Defendants' statements affirming Equifax's compliance with data securing laws were false.

164. Equifax's stock price swiftly declined in response to the news disclosed after the close of trading on September 12, and during trading on September 13. Equifax's stock price closed at \$98.99 per share on September 13, a decline of nearly \$17 per share, or 15%, from its September 12 closing price, on extremely elevated volume of 17.5 million shares traded. According to a September 14, 2017 *Fortune* article, this was the first time since February 2016 that the price of Equifax common stock fell below \$100 per share.

165. Keying off the disclosures in Smith's apology, the market was focused on the financial impact that the 11.5 million subscriptions for free TrustedID service as of that date foretold for Equifax's business. Evercore ISI reported on September 14, 2017, for example:

Since Tuesday, new & negative updates from Equifax and US government agencies increase the uncertainty around future earnings power and substantially raises our estimated cost to EFX of providing free breach services to affected customers for the next year. As a result, we are reducing our [price target] from \$174 to \$110 based on scenario analysis and increasing our forecasted cost to EFX of providing consumers free credit monitoring and identity protection services.

The Evercore report also noted that the free TrustedID enrollment period remained open until November 21, so it was likely that the 11.5 million number reported by Defendant Smith would only rise in the following nine weeks.

4. Revelations Affecting Trading on September 14, 2017

166. Following Equifax's announcement of the Data Breach, though analysts and news outlets speculated as to the cause of the breach and began to quantify the long-term impact on the Company, Equifax itself remained silent as to the precise cause of the hack until nearly a week after its initial announcement.

167. After market close on Wednesday, September 13, Defendants finally disclosed the weakness that resulted in the Data Breach. That night, Equifax updated its breach disclosures to confirm that the vulnerability in its software that led to the Data Breach was a remote code execution vulnerability in the Apache Struts framework known as CVE-2017-5638, and that among those impacted by the Data Breach were customers who signed up for Equifax's credit monitoring services as a protection from identity theft. In a corporate statement posted on the Equifax website, the Company stated:

We know that criminals exploited a US website application vulnerability. The vulnerability was Apache Struts CVE-2017-5638. We continue to work with law enforcement as part of our criminal investigation, and have shared indicators of compromise with law enforcement.

As described in detail *supra*, Section IV(F), the CVE-2017-5638 vulnerability is a dangerous exploit that makes it possible for hackers to force vulnerable systems – like Equifax's systems – to run computer programs written by the hackers which make it simple to steal data.

168. This disclosure notified the market that the Data Breach was not a “zero-day attack” taking advantage of a previously unknown and unreported vulnerability, but rather was the result of a vulnerability in older versions of the Apache Struts software that was identified on March 6, 2017 and for which a patch was made available the following week. Accordingly, this disclosure communicated that Equifax’s data protection infrastructure was so poor that the Company had allowed an easy-to-fix, highly dangerous vulnerability to remain unpatched.

169. Media reports made clear that Equifax’s September 13, 2017 disclosure further indicated significant undisclosed issues with Equifax’s cyber security framework that were inconsistent with the Defendants’ Class Period false and misleading statements (detailed below).

170. As commentary continued into Thursday, September 14, the FTC joined the FBI and the coalition of state attorneys general on the growing list of state and federal politicians and committees investigating Equifax and announced that it was initiating its own investigation into the Company and the Data Breach. Notably, the FTC acting director of public affairs Peter Kaplan stated that while it is not standard protocol to comment on ongoing investigations, the FTC was confirming its investigation into Equifax “in light of the intense public interest and the potential impact of this matter.”

171. Also on September 14, House Oversight and Government Reform Committee Chairman Gowdy (R-SC) and House Science, Space, and Technology

Committee Chairman Lamar Smith (R-TX) sent a letter to Smith requesting documents and a briefing related to the Data Breach. Among other things, the letter stated that “the federal government relies on major credit reporting agencies like Equifax to provide identity verification services. Now, the ability of Equifax to provide such services and secure NPPI has been called into question.”

172. In response to these disclosures, Equifax’s stock price fell another 3.2% on Thursday, September 14, on extraordinarily high volume of 34.58 million shares traded, to close at \$96.66 per share.

173. Analysts also were critical of the underlying facts disclosed by Equifax that a failure to patch a months-old vulnerability for which a patch was available was the cause of the Data Breach, with Macquarie Research writing that the Data Breach

may have ultimately been the result of lax and preventable infrastructure flaws. We are therefore concerned that sensitive data may have been accessible directly from Equifax’s compromised web server; that said sensitive data may not have been encrypted, and note that a certain Equifax employee login portal has since been found to have used default login credentials that were easily guessed.

174. The Macquarie report said further that the “lax oversight” allowing for sensitive consumer data to be stored locally on the public-facing web server that was hacked “is suggestive of further data leakage risk”, and that “a robust web application firewall . . . could have prevented an attacker from exploiting the Apache Struts vulnerability that impacted Equifax, in addition to several other recently disclosed vulnerabilities in Apache Struts.”

5. Revelations Affecting Trading on September 15, 2017

175. After a week of intensifying backlash over a string of disclosures revealing the severity of Equifax's cybersecurity failures, on Friday, September 15, 2017, Equifax issued a press release stating that its Chief Information Officer David Webb and CSO Susan Mauldin were retiring, effective immediately. The same press release stated that "Equifax's internal investigation of [the Data Breach] is still ongoing and the company continues to work closely with the FBI in its investigation."

176. The same day, Equifax announced that the personal details of up to 400,000 U.K. citizens – including names, birth dates, email addresses, and telephone numbers - may have been compromised in the Data Breach.

177. In response to the news disclosed on Friday, September 15, Equifax's stock price dropped another 5% to close at \$92.98, nearly a 36% decline since the Company announced the breach only a week earlier.

178. In the days following Mauldin's resignation, news outlets questioned her role in facilitating the Data Breach. Shortly after the Company disclosed the Data Breach, Mauldin's LinkedIn profile was made private, her credentials showing that she received bachelor's and Master of Fine Arts degrees in music composition were hidden, and her last name was changed to only "M."⁷

⁷ See Appendix, Figure 3.

179. After seeking out further details concerning Mauldin’s credentials and training, journalists learned that she had no relevant education at all, and worse, that Equifax tried to conceal this damaging fact in the face of the Data Breach. Equifax was criticized for its attempts to conceal the fact that Mauldin – Equifax’s *Chief Security Officer* – had no formal security or technology education, what MarketWatch called a “lack of educational qualifications” for her job.

H. Post-Class Period Developments

1. Smith Departs the Company Without Severance

180. On September 26, 2017, Equifax announced Smith’s retirement, effective immediately. The Board took the unusual step of announcing that it had the power to retroactively classify Smith’s departure as termination for cause, allowing the Company to initially claw back some of the extraordinary compensation Smith received during the time he oversaw Equifax’s wretched data protection infrastructure and allowed it to fall into utter disrepair.⁸ Notably, “cause” is narrowly defined in Smith’s employment agreement as: (a) a guilty or no-contest plea to a felony or “crime involving moral turpitude”; (b) an intentional violation of Equifax’s ethics or insider-trading policies; (c) or a failure to do his job in a “willful

⁸ According to Equifax’s Annual Report filed with the SEC on Monday, April 2, 2018, Smith will bring home a total \$15.7 million in compensation for 2017, a 4.9% increase from the previous year. Much of this increase is due to a \$1.4 million stock option award.

and continued” fashion. Smith retired without severance, and was denied his annual bonus opportunity for 2017.

2. Defendants Have Now Admitted that There Were Numerous Serious Deficiencies in Equifax’s Data Security Posture

181. Since the end of the Class Period, Equifax has admitted that there were numerous deficiencies in its cybersecurity that persisted throughout the Class Period, and acknowledged that serious remedial efforts are required to address them. A November 9, 2017 *New York Times* article reported that Equifax’s ongoing internal investigation into the Data Breach had “already uncovered ‘*two significant deficiencies*’ in the company’s technology systems that are being remediated[.]”

182. Significantly, as discussed above, Smith admitted in response to a question from Representative Robert Pittenger that Equifax did not have “preventative measures in place to combat a breach of this magnitude.” Specifically, Smith stated, “*Well, obviously a breach of this magnitude would not have occurred if everything was – was in place.*” Likewise, in response to questioning from Senator Maria Cantwell, Smith admitted that the Data Breach occurred because “basic [cybersecurity] hygiene issue wasn’t followed.” And, in testimony before the Senate Commerce Committee, interim CEO Barros admitted that Equifax had failed to fulfill its obligation to protect consumer data during the Class Period. Barros testified, “Our top job must be to protect the data entrusted to us. *We did not meet the public expectations* and now it’s up to us to prove that we can regain the trust.”

183. Equifax has described the significant efforts it is now belatedly taking to overhaul its cybersecurity systems, making clear just how little protection was actually in place during the Class Period, contrary to Defendants’ reassuring misstatements. For instance, on November 8, 2017, the *Wall Street Journal* reported that an Equifax spokesperson told the paper that “Equifax is in the process of ‘*either encrypting or deleting*’ data stored on its computer storage systems Since the breach, ‘Equifax has deployed multiple methodologies to strengthen security and protect data[.]’” Equifax’s admission makes clear that the Company was still maintaining legacy data on its live databases that *should have been deleted but was not*, creating an unreasonable cybersecurity risk, and the Company *systematically failed to encrypt* sensitive data that was still used to provide client services.

184. Likewise, at a Senate Commerce Committee hearing, Barros testified that after the Data Breach was announced, Equifax finally brought its patching capabilities “up-to-speed” and implemented security redundancies that should have been in place from the start. Barros testified that Equifax performed

a comprehensive review on the process, improving our patching capabilities, improving our tools, updating our tools, making sure that our detecting process is *much more up-to-speed at this stage*. We have changed the policies to making sure that *we have redundancies and closed loops in place*, you know, to improve the accuracy and precision of execution.

At the same hearing, Smith testified, “The entire environment in which this criminal attack occurred is now **much different**. It’s a **more modern** environment with **multiple layers of security that did not exist before**.”

185. Similarly, during Equifax’s third quarter 2017 earnings call, Barros made clear that the Company was just beginning to put basic security measures into place that should have been implemented long before the Data Breach occurred. Barros stated that Equifax was

hardening [its] networks, changing our procedures to require closed-looped confirmation when software patches are applied, rolling out new vulnerability scanning tools and processes, and increasing accountability mechanisms for our security and IT team members *We’re also working to bolster our security culture throughout the entire company.* Data security will be a mandatory responsibility for all Equifax employees I have revised our corporate governance structure so that Equifax’s Chief Security Officer reports directly to [the CEO].

186. Since the Data Breach, Equifax has been forced to ***quadruple*** its spending on cybersecurity to bring it into reasonable compliance with industry standards and the mandates of applicable data security laws, demonstrating that the Company’s spending on cybersecurity during the Class Period was inadequate. As Senator Warren’s report explains, “despite record profits in recent years, Equifax spent only a fraction of its budget on cybersecurity – approximately 3 percent of its operating revenue over the last three years.”

187. Said another way, while Equifax spent more than \$2.37 billion between 2014 and 2016 to acquire new companies so it could obtain more consumer data, it spent approximately one tenth of that amount to protect the data it had in hand. Accordingly, on Equifax's third quarter 2017 earnings call, Barros told investors that Equifax would spend an additional \$20 million to \$25 million on cybersecurity in fourth quarter of the year alone, which Gamble referred to on that same call as "up dramatically from what it has been in the past," with spending increasing in 2018. In his testimony before Congress, Barros explained that the increased spending was essential to ensure Equifax was appropriately protecting the data entrusted to it:

[W]e believe that today we are better than we were at the time of the breach for one reason: This was a pivoting point in our industry. We had to, in our company, essentially, we have to make significant investments, and will continue to do so to make sure that it [is] better today, and will be better tomorrow.

188. Notably, in its 2017 Form 10-K filed with the SEC on March 1, 2018, Equifax acknowledged that its cybersecurity systems are currently inadequate to protect the Company from a large-scale data intrusion and that additional remediation is required. Equifax stated, "Following the [Data Breach], we began undertaking significant remediation efforts and other steps to enhance our data security infrastructure . . . but *there will be additional changes needed to prevent a similar incident*" – a disclosure the Company should have issued by the very start of the Class Period. Likewise, Equifax's 2017 Form 10-K further stated that the Company's "information technology networks and infrastructure . . . *are vulnerable*

to unauthorized access to data or data breaches of confidential information.”⁹ Unfortunately for investors, Equifax finally issued these important disclosures far too late.

189. Similarly, in its proxy statement filed on April 2, 2018, Equifax reported that because of the data breach, its “senior leadership team would not receive annual cash incentive compensation for 2017 even though performance measures were achieved.” According to the Proxy, Equifax “added a cybersecurity performance measure as one of the metrics to evaluate performance of all employees, including [the Company’s] executives, under the 2018 annual bonus plan[,]” and “will no longer grant performance shares tied to three-year cumulative Adjusted EPS to avoid providing any incentive to limit spending on cybersecurity.”

190. On March 14, 2018, the SEC and the United States Attorney for the Northern District of Georgia named Jun Ying, the former CIO of Equifax’s largest business unit – USIS – in complaints alleging civil and criminal insider trading violations. Ying sold \$1 million worth of his Equifax shares on August 29, 2017 immediately upon determining that Equifax had been the subject of a data breach – just days before that information was disclosed to the public.

191. Ying’s sales were the product of his personal research into the impact other reported data breaches had on the price of those companies’ publicly traded

⁹ By contrast, during the Class Period, Defendants stated that Equifax’s networks “**could be** vulnerable to damage disruptions, shutdowns, or breaches of confidential information due to criminal conduct.”

shares. The charges against Ying lay bare that in the aftermath of the Data Breach, Equifax executives were far more concerned with controlling the message and information about the Data Breach than they were in fixing, disclosing and responding to it. For example, before learning of Ying's insider trading, Equifax had determined to offer Ying the job as CIO of the entire Company, but did not even bring him into the plans to respond to the Data Breach until late August 2017, and even then only told him, and other senior executives, that they had an "all hands" situation involving a *data breach at a customer*.

192. Finally, on March 28, 2018, Equifax appointed private equity executive Mark Begor as CEO. In his initial comments to the public regarding his role at the Company, Begor admitted that, contrary to Defendants' public representations to investors during the Class Period, the Data Breach was the result of Equifax not having the "right defenses in place":

We didn't have the right defenses in place, but we are investing in the business to protect this from ever happening again. . . . We are a public trust in many regards and we need to work to earn that trust back.

3. Equifax's Data Protection Measures Are Severely Criticized by Experts, Lawmakers, and Others

193. In the wake of the disclosures discussed above, Equifax's profoundly inadequate data protection measures and lax security practices have been categorically and vociferously condemned by cybersecurity experts, lawmakers, and others. For instance, at an October 5, 2017 hearing of the House Financial Services Committee, Representative Maloney called Equifax's failure to implement

reasonable data protection measures, “*the most open-and-shut violation of the Safeguards Rule that I have ever seen in the history of this country*” At that same hearing, Representative Blaine Luetkemeyer stated that Equifax’s senior leadership was directly responsible for the Company’s poor cybersecurity, characterizing its failure to implement appropriate data protection measures as “*disregard for the law* and for consumers. There’s a failure on the part of [Equifax], your board and your senior management.” At a Senate Banking Committee hearing on October 4, 2017, Senator Warner stated, “The fact that there was known vulnerability, that you didn’t have appropriate internal controls in place to easily patch this is *inexcusable*.”

194. Moreover, the Warren Report found that Equifax “ignored numerous warnings of risks to sensitive data” before the Data Breach occurred, and had “set up a flawed system to prevent and mitigate data security problems.” Importantly, the Warren Report noted Equifax’s duty to disclose material information to investors, and found that “[a]fter first learning of suspicious activity on its network, Equifax *waited 40 days to inform investors*.” The report also noted that Defendants missed “key opportunities to inform investors of risks,” including the August 16, 2017 presentation described above. The report concluded that “*Equifax neglected their duty to investors by failing to inform them of the breach during that [August 2017] presentation, and continued to withhold material information that had a large impact on the company for more than three weeks*.”

195. SEC Commissioner Jay Clayton made similar statements at a September 26, 2017 Senate Banking Committee hearing. Commissioner Clayton was asked whether he believed Equifax’s disclosures to investors were adequate. While declining to comment on the behavior of individual companies, Clayton said, “Companies should be providing *better disclosure about their risk profile*; companies should be providing *sooner disclosure about intrusions that may affect shareholders’ investment decisions*.”

196. Shortly thereafter, on February 26, 2018, the SEC issued Release Nos. 33-10459; 34-82746, “Statement and Guidance on Public Company Cybersecurity Disclosures,” the substance of which is a clear rebuke of Equifax’s disclosures to investors during the Class Period. The SEC emphasized that

it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack.

The SEC explained that it “expect[s] companies to provide disclosure that is tailored to their particular cybersecurity risks and incidents.” Among other things, issuers are required to disclose “the probability of the occurrence and potential magnitude of cybersecurity incidents,” and “the adequacy of preventative actions taken to reduce cybersecurity risks.” The SEC cautioned that “boilerplate language” is insufficient to warn about the specific risks and inadequacies associated with an issuer’s cyber-defenses. With respect to issuers’ obligation to timely disclose a data

breach, the SEC made clear that “an ongoing internal or external investigation – which often can be lengthy – would not on its own provide a basis for avoiding disclosures of a material cybersecurity incident.” In an obvious reference to Gamble’s and Ploder’s insider sales, the SEC went out of its way to state that insiders “must not trade a public company’s securities while in possession of material nonpublic information, which may include knowledge regarding a significant cybersecurity incident experienced by the company.” The SEC stated that an issuer fails to meet its obligation under the Sarbanes-Oxley Act to maintain effective internal controls over reporting where, like Equifax, it lacks an adequate process for monitoring and publicly reporting cybersecurity risk, such as data breach plan that facilitates swift public disclosure of a breach. Finally, the SEC “remind[ed] companies that they may have a duty to correct prior disclosure” about cybersecurity risks “that the company determines was untrue (or omitted a material fact necessary to make the disclosure not misleading) at the time it was made.”

197. The Data Breach has also spurred significant new legislative efforts to ensure that data aggregators adequately secure consumer information. On October 12, 2017, deputy GOP whip Representative Patrick McHenry introduced a bill requiring the three major credit firms to submit to regular cybersecurity reviews. The “PROTECT Act” – Promoting Responsible Oversight of Transactions and Examinations of Credit Technology Act – would also create uniform cybersecurity standards for credit bureaus and submit them to onsite examinations.

198. Cybersecurity experts were also in agreement that the scope and magnitude of the Data Breach demonstrated that Equifax had systemically failed to implement a reasonable data security regime. For instance, a September 7, 2017 *New York Times* article quoted cybersecurity expert Avivah Litan as saying that “‘Equifax should have multiple layers of controls’ so if hackers manage to break in, they can at least be stopped before they do too much damage.”

199. Likewise, *Wired* reported in a September 24, 2017 article:

The accumulation of missteps, slow disclosure, and problematic public response with so many millions of innocent consumers potentially affected *deeply troubles security practitioners* And the more recent mistakes join a list of other revelations that Equifax *had a disorganized approach to security, and a naiveté about the possibility of a breach*. The fact that attackers got into Equifax’s systems through a known vulnerability with a patch available galls security analysts. But the company also acknowledged that it knew about the patch when it was first released, and had actually attempted to apply it to all its systems. This inadequate effort hints at *the truly haphazard nature of Equifax’s operation*.

200. The *Wired* article quoted cybersecurity expert Jason Glassberg, cofounder of the corporate security and penetration testing firm Casaba Security, as stating, “Equifax sits on the crown jewels of what we consider personally identifying information. You’d think a company like that, guarding what they’re guarding, would have a heightened sense of awareness and that clearly was not the case.”

201. Additionally, the ICIT, a leading cybersecurity think tank underwritten by KPMG, MasterCard, Symantec, BitSight Technologies and other corporate giants, issued a report finding that “[a] catastrophic breach of Equifax’s systems was

inevitable because of *systemic organizational disregard for cybersecurity and cyber-hygiene best practices*, as well as Equifax’s reliance on unqualified executives for information security.”

202. At a November 1, 2017 Congressional hearing, noted cybersecurity expert Bruce Schneier testified:

Equifax was solely at fault. This was not a sophisticated attack. The security breach was a result of a vulnerability in the software for their websites: a program called Apache Struts. The particular vulnerability was fixed by Apache in a security patch that was made available on March 6, 2017. This was not a minor vulnerability; the computer press at the time called it ‘critical.’ Within days, it was being used by attackers to break into web servers. Equifax was notified by Apache, US CERT, and the Department of Homeland Security about the vulnerability, and was provided instructions to make the fix. Two months later, Equifax had still failed to patch its systems. It eventually got around to it on July 29. The attackers used the vulnerability to access the company’s databases and steal consumer information on May 13, over two months after Equifax should have patched the vulnerability.

* * *

This is not the first time Equifax failed to take computer security seriously. It confessed to another data leak in January 2017. In May 2016, one of its websites was hacked, resulting in 430,000 people having their personal information stolen. Also in 2016, a security researcher found and reported a basic security vulnerability in its main website. And in 2014, the company reported yet another security breach of consumer information. There are more.

203. Finally, the Apache Software Foundation, developer of Apache Struts, issued a statement noting that “any complex software contains flaws,” and, therefore,

responsible users will establish “security layers” behind a public-facing presentation layer such as the Struts framework. *“A breach into the presentation layer should never empower access to significant or even all back-end information resources.”*

4. Equifax’s Business Continues to Experience Significant Harm As a Result of the Data Breach

204. Equifax continues to experience significant ongoing harm to its business because of the Data Breach. As a September 15, 2017 *Wall Street Journal* article explained that the Data Breach was likely to be one of the “most expensive” in history and that its costs could weigh on the Company for “years to come.”

[R]esearchers who have studied similar incidents say the size and sensitive nature of the information involved in Equifax’s breach means it could shape up to be one of the most expensive breach recoveries in history. The clear and immediate costs such as notifying victims, hiring a firm to do a forensic investigation, legal fees, and fines as well as hard-to-calculate costs such as lost business, reputational damage, and insurance premium increases, will likely weigh the firm down for years to come, said Dana Simberkoff, a compliance expert at the software firm AvePoint Inc.

205. In the third quarter of 2017 *alone*, Equifax incurred \$87.5 million in one-time charges related to the Data Breach, including legal costs, cyber forensic investigation expenses and the cost of providing free credit-monitoring services to consumers. That last charge totaled **\$60.2 million** in the third quarter, and the Company explained that it expected to spend up to an additional \$110 million to continue providing that service. On Equifax’s third quarter earnings call, Gamble stated that, in the fourth quarter alone, the company expected to incur around \$60

million to \$75 million in breach-related costs, including increased spending on IT and security, with expenses continuing indefinitely in 2018.

206. Equifax has also continued to experience serious blowback from its customers. On the Company's third quarter 2017 earnings call, Barros and Gamble stated that Equifax was seeing "deferrals of customers' decisions regarding the purchase of new products or discrete products and services in [the] third quarter and fourth quarter to date" across numerous business lines. Barros stated that customers "want to make sure that our security systems are in line with their expectations We're hoping to win back their trust and then be able to regain that business that we've indicated has been deferred, and we're still working through that process."

207. To date, Equifax has been named in approximately 240 consumer lawsuits arising from the Data Breach. Equifax's third quarter 2017 Form 10-Q acknowledges that "it is reasonably possible that we will incur losses associated with these proceedings and investigations."

I. Equifax's Data Protection Measures Were Grossly Inadequate, and Failed to Meet Either Basic Industry Standards or Applicable Legal Requirements

208. As discussed above, Defendants knew or recklessly disregarded that Equifax's data protection measures were grossly inadequate to protect the sensitive data in its custody, failed to meet the most basic industry standards, and ran afoul of the well-established mandates of applicable data protection laws, including the Safeguards Rule.

1. Equifax Failed to Implement an Adequate Patch Management Process and Routinely Failed to Address Known Vulnerabilities

209. Equifax failed to implement an adequate patch management process and failed to remediate known deficiencies in its cybersecurity infrastructure. As discussed above, Equifax relied on a single individual to manually implement the Company's patching process across the entirety of its vast network. This individual did not know, and apparently had no way of knowing, where vulnerable software was being run and where patching needed to be implemented. The process ran without adequate closed-loop redundancies and oversight, and was far behind the automated patching processes that Equifax's peers – and even companies that do not store highly valuable private information – implemented. As a testament to the inadequacy of this process, it took Equifax almost five months to finally patch the highly dangerous Apache Struts vulnerability, even though the vulnerability had been widely publicized and individualized notice from DHS had been provided to Equifax. Moreover, as discussed above, Equifax failed to timely and adequately address deficiencies reported by security researchers, consultants, and others, including serious XSS and forced browsing vulnerabilities.

210. Equifax's patching processes failed to satisfy basic industry standards. Promptly applying security patches is a necessary and critical cybersecurity practice, and one experts consider to be the single most effective data protection measure. *See, e.g.*, NIST Special Publication 800-53r4 (published in 2013, well before the

start of the Class Period). According to a peer-reviewed study presented at the 2015 Symposium on Usable Privacy and Security, “When asked for the top three things they do to stay safe online, the most common response from experts was installing software updates.” Indeed, Equifax’s security terms of service, posted on its website, required users of its services to agree that “[a]ll servers must be kept current with appropriate security-specific system patches, as they are available.” NIST’s standards require organizations to “[i]nstall . . . security-relevant software and firmware updates,” and specifically direct them to make use of “available resources such as the . . . Common Vulnerabilities and Exposures (CVE) database[,]” on which the Apache Struts vulnerability was prominently published. Promptly applying software updates is so important that NIST SP 800-53 requires that it be implemented for all organizational systems, without regard to the sensitivity of the information stored therein. Prompt and effective application of patching and updates is even more critical when a system is used to store sensitive information.

211. However, as cybersecurity experts have explained, Equifax’s patching processes failed to meet these standards. Cybersecurity expert Amit Yoran, for example, wondered how Equifax could honestly believe it exercised “a reasonable standard of care” with respect to a patch process “where the entire cyber infrastructure of Equifax and securing access to all of this incredibly sensitive information about hundreds of millions of people boil down to one person.” Likewise, at the November 8, 2017 Senate Commerce Committee hearing, Todd

Wilkinson, CEO of a cybersecurity company, compared having a patching process that quickly and reliably addresses vulnerabilities to putting “locks on your front door Good cyber hygiene includes things like reacting quickly to zero-day threats.” Commenting on Senator Peters’ observation that the Data Breach “was a simple hack because the road map was pretty much put out for folks to take,” Wilkinson explained that this is precisely why reliable patching processes are an essential element of basic cybersecurity: “the need to respond quickly to close down those types of threats in your ecosystem is very, very important Again, it’s basic – it’s best practices, it’s hygiene.”

212. Moreover, while both NIST standards and the CIS Critical Security Controls standards, version 6 (“CIS”), published by the SANS Institute in 2015,¹⁰ characterize the maintenance of a comprehensive inventory of assets (*e.g.*, software, devices) as a fundamental, “baseline” security requirement,¹¹ Smith’s concession that the single individual responsible for administering Equifax’s patching process

¹⁰ The SANS Institute is an organization specializing in cybersecurity training. SANS developed a set of cyber-defense standards – the CIS – in partnership with U.S. National Security Agency cyber-teams, U.S. Department of Energy specialists, law enforcement agencies, and top forensic consultants. According to SANS, the CIS have been “vetted across a very broad community of government and industry practitioners.”

¹¹ Indeed, CIS characterizes such an inventory as among the “First 5 CIS Controls,” which “[e]liminate the vast majority of your organization’s vulnerabilities.”

did not know, and had no way to readily determine, which systems ran Apache Struts demonstrates that Equifax failed to maintain such an inventory.

213. As alleged above, Equifax received repeated warnings, both before and during the Class Period, that its patching processes fell well short of basic cybersecurity standards. Among other things: (1) a 2016 Deloitte audit found several problems with Equifax's cybersecurity, including a "careless approach to patching systems"; (2) former Equifax employees stated that Equifax had a long history of failing to adequately patch vulnerabilities, which led to serious compromises of data security; (3) as part of a March 2017 investigation that Smith personally supervised, "Mandiant warned Equifax that its unpatched systems and misconfigured security policies could indicate major problems"; and (4) non-public analyses by cybersecurity firms showed that "weaknesses in Equifax's security systems were apparent in the months before" the Data Breach, and, in particular that Equifax's patching process fell below industry standards.

214. Equifax's patching processes also failed to comply with applicable data protection laws, including the Safeguards Rule. As Representative Maloney explained at the October 5, 2017 House Financial Services committee hearing, "The Safeguards Rule also requires you to have a patch management system; essentially, a system in place to patch security flaws as soon as a fix for the flaw is released." Indeed, the FTC made clear, well before the start of the Class Period, that a failure to implement an appropriate patching process violates the Safeguards Rule and the

FTC Act. *See, e.g., In the Matter of Fajilan and Associates, Inc.*, 2011 WL 11798456, at *3 (F.T.C. August 17, 2011) (corporate defendant’s failure to “identify and patch vulnerabilities” and “take appropriate action to correct existing vulnerabilities or threats to personal information in light of known risks” violated the Safeguards Rule); *In the Matter of LabMD, Inc.*, 2014 WL 2142681, at *6 (F.T.C. May 6, 2014) (failure to “patch software” and “update operating systems” violates the FTC Act). In particular, the FTC has explained that “[m]aintaining and updating operating systems of computers and other devices to protect against known vulnerabilities is integral to a company’s defense in depth strategy.” *Id.* at *7; *see also In the Matter of GUESS?, Inc. and GUESS.com, Inc.*, Case No. C-4091 (C.D. Cal. 2003) (failure to protect website against commonly known vulnerabilities, including SQL injection, violates the FTC Act). Likewise, in agency guidance published in 2015, the FTC stated, “Outdated software undermines security. The solution is to update it regularly . . . having a reasonable process in place to update and patch third party software is an important step to reducing the risk of a compromise.”

215. State data protection laws also require the implementation of a reliable patching process. As discussed above, Massachusetts data protection regulations provide, “For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the

personal information.” 201 C.M.R. 17.04(6); *see also In re Verizon Related Reduction Claim*, N.Y. Pub. Servs. Comm’n, Docket No. 99-C-0949 (May 29, 2003) (by failing to test and apply security patches, Verizon failed to take reasonable precautions to address a known vulnerability).

216. Foreign law imposes the same requirement to implement a reliable patching process and ensure software and systems are promptly updated. For instance, the U.K. Data Protection Act of 1998 and the EU Data Protection Directive both require organizations to “apply security updates as soon as they are made available.” The U.K. Data Protection Act of 1998 further cautions that “[a]ttackers typically run automated scans . . . searching for un-patched, out-dated or otherwise vulnerable software to attack. It is therefore important that any software you use to process personal data is subject to an appropriate security updates policy.”

2. Equifax Failed to Encrypt Sensitive Data

217. Equifax failed to implement adequate encryption measures to protect sensitive consumer and employee information in its custody during the Class Period. Equifax has admitted that troves of sensitive personal information residing in its systems, relating to hundreds of millions of Americans, were not encrypted, but rather were stored in plaintext, making it easy for intruders to read and misuse. These data were not encrypted despite the fact that they were accessible through a public-facing, widely used website, enabling any attacker that compromised the website’s server to immediately access that sensitive data. In testimony before

Congress, Smith further admitted that even with respect to its core credit databases, Equifax failed to encrypt *any* of its data. And, even in cases where Equifax did encrypt sensitive data, it recklessly left the keys to unlock that encryption on the same public facing networks during the Class Period, even though the Company had been notified prior to the start of the Class Period that this practice was occurring.

218. Incredibly, Equifax even failed to encrypt highly vulnerable mobile applications. Equifax was ultimately forced to remove these mobile applications from the Apple Store and Google Play at approximately the same time it announced the Data Breach because the applications “suffered from numerous vulnerabilities that allowed for man-in-the-middle and other attacks.” In other words, not only was Equifax failing to encrypt sensitive data stored on its systems, it failed to encrypt such data as it was being sent on the internet – a profound security failure. Jerry Decime, the researcher who notified Equifax that its mobile applications were not encrypted, stated, “They quite frankly didn’t know what they were doing.”

219. Equifax’s inadequate encryption protocols fell far short of basic industry standard security practices. For example, at the November 8, 2017 Senate Commerce Committee hearing, Senator Gardner asked “the privacy experts” whether it was “a reliable, safe methodology to leave [the sensitive consumer information that was stolen in the Data Breach] unencrypted at rest.” Wilkinson, one of those experts, responded that encryption at rest was “a very important [tool] to be used for data of this type [*i.e.* of the type that Equifax maintained, failed to

encrypt, and was ultimately stolen] that is of high value.” Wilkinson proceeded to explain that Equifax’s peers and “[o]ther segments of the industry” impose “requirements that requires this kind of information – credit card data at retailer and thing like that – to be encrypted.”

220. Indeed, the PCI (Payment Card Industry) Standards, which set forth standards for payment data, require that sensitive data must “be unreadable anywhere it is stored.” In addition, NIST SP 800-53r4 provides that encryption of data at rest is in an “initial control baseline,” *i.e.*, a “starting point,” in determining security controls for “moderate and high-impact” information systems, like those containing sensitive personal information. NIST standards further provide that the “strength of [cryptographic] mechanism [used to protect stored data] is commensurate with the security category and/or classification of the information.” Given the extremely sensitive nature of the data Equifax maintained, those data should have been afforded the strongest cryptographic protections.

221. In addition, PCI Standards require that organizations “verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls).” Equifax’s practice of storing encryption keys in the same place as the encrypted data those keys unlocked failed to satisfy that standard.

222. By failing to adequately encrypt the sensitive information, Equifax failed to comply with applicable data security laws. Even before the start of the

Class Period, the FTC made clear that it is improper to store sensitive data in unencrypted on internet servers that might be publicly accessible. For instance, in *LabMD*, the FTC alleged that the defendant company had “engaged in fundamental, systemic security failures that put at risk consumers’ sensitive personal and health information” where it “did not encrypt Personal Information while it was maintained on its network,” and violated the FTC Act where personal information was “stored in an unencrypted format.” The Commission agreed, finding that the company’s “security practices were unreasonable, lacking even basic precautions to protect the sensitive consumer information maintained on its computer system.” *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 256, 258 (3d Cir. 2015) (storing unencrypted credit card data and other sensitive information violates the FTC Act).

223. Additionally, as noted above, state data protection laws also required Equifax to encrypt the personal information it maintained. Massachusetts regulations, for instance, require that any company that collects or maintains sensitive personal information implement a written information security program, which must include encryption of that personal information. 201 CMR § 17.02.

3. Equifax Failed to Implement Adequate Authentication Measures

224. As discussed above, “authentication measures” are mechanisms such as passwords used to verify that a party attempting to access a system or network is authorized to do so. Equifax’s authentication measures, including weak passwords and security questions, were inadequate to protect the sensitive data in the

Company's custody. For example, Equifax relied on four digit pins comprised of Social Security numbers and birthdays to guard personal consumer and employee information, even after such "passwords" had been compromised in prior hacks and after the Company had explicitly represented that it would refrain from using authenticators based on personal identifiers.

225. Likewise, Equifax "protected" one of its portals used to manage credit disputes with the username 'admin' and password 'admin.' This portal allowed access to a vast cache of personal information, including employee names, emails, usernames, passwords, consumer complaint records, and the Argentinian equivalent of Social Security numbers. The portal also granted administrative access allowing intruders to add, delete, or modify records. A November 15, 2017 article in *Forbes* quoted cybersecurity expert Wes Moehlenbruck, who stated that this was one of many "very grossly negligent security practices" at Equifax. The article continued, "'Admin/admin' as a database password is a ***surefire way to get hacked almost instantly,***" Moehlenbruck says. 'A production database with this account smells of ***poor security policy and a lack of due diligence.***'"

226. Equifax's authentication measures fell far short of standard security practices, which include the deployment of multi-factor authentication. Multi-factor authentication requires a user to authenticate a password via an additional channel, such as email. As Moehlenbruck explained to *Forbes*, multi-factor authentication

“is common practice now on banking websites, email accounts, and social media. We’re all surprised that a company the size of Equifax isn’t current with the times.”

227. Likewise, NIST standards not only call for implementation of multi-factor authentication, but recommend deploying it “at the application level, when necessary, to provide increased information security.” In other words, under cybersecurity best practices, Equifax should have (but failed to) checked multifactor credentials repeatedly in sensitive applications.

228. Even more fundamentally, Equifax’s use of four-digit pins, particularly those comprised of personal identifiers, to protect sensitive data violates a host of cybersecurity standard practices, including NIST 800-53r4, which requires organizations to “Ensur[e] that authenticators have sufficient strength of mechanism for their intended use.” Four-digit PINs are inherently weak; there are only 10,000 possible 4-digit PINs, and it would be trivial for a computer to try each permutation and access the “locked” system by brute force. Moreover, standard cybersecurity practice calls for authenticators to be based on information that is generally known only to an authorized user; accordingly, a PIN or other password comprised of a user’s birthday is a wholly inadequate authenticator.

229. Equifax’s authentication measures also ran afoul of applicable data protection laws. The FTC Act requires companies to “use common, effective authentication-related security measures,” and “have policies that impose minimum requirements for passwords (*e.g.*, length, required characters, change intervals) to

ensure they are strong.” *LabMD*, 2014 WL 2142681, at *6. In *LabMD*, the FTC cited an employee’s use of a username consisting of her first initial and last name (“sbrown”) and a password that was the name of the company (“labmd”) – identifiers at least as strong as “admin/admin” used by Equifax – as far too weak to satisfy the requirements of the FTC Act. *Id.*; see also *Wyndham*, 799 F.3d at 258 (defendant violated the FTC Act where it “[d]id not employ common methods to require user IDs and passwords that are difficult for hackers to guess[.]”)

230. The FTC has also explained that federal data protection laws require companies to ensure that adequate authentication measures are implemented with respect to *all* end users of networks on which sensitive data are stored, not just with respect to the company’s in-house employees. Thus, the FTC has explained that a company violated the FTC Act when it “routinely created weak passwords for the user accounts it created for computers that it placed in its . . . clients’ offices” – just as Equifax did with respect to the W2Express and TALX breaches (and, unbeknownst to investors, continued to do). Indeed, the FTC has explained that “requir[ing] consumers to choose strong passwords when setting up their accounts . . . is standard practice for accounts containing sensitive personal information.” *In the Matter of TaxSlayer LLC*, 2017 WL 5477618, *4 (F.T.C. Oct. 20, 2017) (company violated Safeguards Rule where its “only requirement for [end users’] passwords was that they be eight to sixteen characters in length.”).

4. Equifax Failed to Adequately Monitor Its Networks

231. Both before and throughout the Class Period, Equifax chronically failed to adequately monitor, and establish mechanisms for monitoring, its systems and networks. For instance, as a former employee in Equifax's IT department told *Motherboard*, Equifax failed to maintain activity logs, set up processes for tracking malicious scripts, or implement "file integrity monitoring" – "not even on systems with sensitive information." The Warren Report similarly concluded:

Equifax neglected the use of robust logging techniques that could have allowed the company to expel the hackers from their systems Logging is a simple but crucial cybersecurity technique in which companies monitor their systems, continuously logging network access in order to identify unauthorized users.

Indeed, Equifax's systems monitoring was so poor during the Class Period that it failed to identify 2.5 million victims of the Data Breach until March 2018, **more than 7 months** after Defendants first claim to have learned about incident.

232. Equifax's failure to adequately monitor its systems greatly compounded the magnitude of the Data Breach. Indeed, as numerous cybersecurity experts have explained, Equifax could not have experienced an intrusion as catastrophic as the Data Breach if it had implemented adequate systems monitoring.

Cybersecurity expert George Hulme noted in *Security Boulevard*:

Equifax could certainly have identified the breach had they been looking more closely at application, server, and security device logs. Network monitoring could have picked up data exfiltration across the network [T]he breach of a single server is something a company

should anticipate – especially a company such as Equifax – so they should have been on continuous lookout for indicators of compromise.

Likewise, a report issued by cybersecurity think tank the ICIT explained:

Data loss prevention is the employment of reliable vendor tools to secure data when it is in transit, when it is at rest, and when it resides at endpoints. DLP governs which data end users can transfer and which data can leave the network Equifax should have been suspicious of the amount of consumer traffic leaving its network, the prolonged activity of that traffic egress, and the external destination of millions of consumer data sets. *If Equifax had invested in or licensed a DLP solution, automatic rules configured by a trained information security team would have prevented any internal or external threats from exfiltrating sensitive consumer data from the network.*

Similarly, the Warren Report found that “Equifax allowed hackers to continuously access sensitive data for over 75 days, in part because the company failed to adopt effective logging techniques and other security measures.”

233. Equifax failed to employ security best practices with respect to systems and network monitoring, especially for a company that maintains data as valuable as those maintained by Equifax. Logging and monitoring network access is so fundamental to adequate data security that CIS provides that “Maintenance, Monitoring, and Analysis of Audit Logs” is one of the six most basic steps an organization must take to safeguard data. Likewise, NIST SP 800-53r4 contains 14 pages of detailed recommendations about how to correctly store, capture, and audit logs from systems. NIST specifies that inbound and outbound traffic should be monitored in *real time* by automated tools with respect to systems containing

sensitive information. That Equifax failed to perform adequate network logging and monitoring is shocking given the value of the data with which they were entrusted.

234. The Safeguards Rule requires financial institutions to implement adequate policies and procedures for monitoring and tracking suspicious activity on its networks. *In the Matter of Franklins Budget Car Sales, Inc.*, 2012 WL 2150214, at *2 (F.T.C. June 7, 2012) (violation of Safeguards Rule where company failed “to prevent, detect, and investigate unauthorized access to personal information” including by not “inspecting outgoing transmissions to the internet.”); *In the Matter of ACRA Net, Inc.*, 2011 WL 11798455, at *11 (F.T.C. Aug. 17, 2011) (organizations must adopt “an effective system” for “monitoring to detect anomalies and other suspicious activity” in their systems). The FTC Act requires companies custodying personal information “implement reasonable steps to maintain an effective system of monitoring access” to their systems, “including by monitoring to detect anomalies and other suspicious activity.” *Fajilan*, 2011 WL 11798456, at *3; *see also LabMD*, 2014 WL 2142681, at *8 (inadequate logging protections violate the FTC Act).

5. Equifax Allowed Sensitive Data to be Easily Accessed On Public-Facing Servers and Also Failed to Partition It

235. In contravention of both data security best practices and data protection laws, Equifax stored and maintained sensitive personal information so that it was accessible (in unencrypted, plaintext form) through public-facing servers and web portals, and failed to partition sensitive data so as to limit exposure in case of a breach. As a direct result of these improper practices, the hackers behind the Data

Breach gained access to a vast trove of sensitive consumer information merely by exploiting a vulnerability in a web application relating to a public dispute portal. Equifax was warned by security researchers well in advance of the Data Breach, including in December 2016, that sensitive consumer and employee information in its custody was publicly accessible and vulnerable to theft and misuse.

236. Standard security practices call for companies to ensure that sensitive data is stored on non-public servers and is otherwise inaccessible through public-facing networks. This flows from a fundamental principle of cybersecurity: to ensure that no system has a “single point of failure” – a vulnerability that if compromised, would jeopardize the entire system.

237. Indeed, Equifax’s own security terms of service provide that users of its portals must ensure that “[s]ervers storing Equifax Information must be separated from the Internet or other public networks by firewall or other comparable methods” and that “Equifax Information must not be stored on a server that can be accessed by TCP services directly from the Internet and should not be referenced in domain name services (DNS) tables.” Astonishingly, Equifax itself clearly failed to comply with these directives.

238. Likewise, cybersecurity experts have explained that Equifax’s failure to employ adequate network segmentation was grossly inconsistent with standard cybersecurity practices. For instance, the ICIT explained:

Network segmentation is the practice of dividing a network into smaller partitions, called subnets, to isolate critical assets from one another and

control access to sensitive data Network segmentation prevents lateral compromise. *If Equifax had properly segmented its network, then the attackers would not have been able to access consumer data via the public-facing web portal.*

The *Wall Street Journal* similarly reported in a September 18, 2017 article:

Some people in the credit-reporting and information-security industries say Equifax appeared to be using a centralized system for some data, which might have made its information more vulnerable. Other companies have moved to systems that spread out consumers' personal data in different places. If there is a security breach, the chances of hackers getting all the data in one swoop are much lower, the people added.

239. Likewise, NIST standards provide that an information system should be “partition[ed as] part of a [standard] defense-in-depth protection,” and that organizations should “restrict or prohibit network access and information flow among partitioned information system components.”

240. Equifax's storage of vast quantities of sensitive consumer information without any network segmentation ran afoul of data protection laws. *Wyndham*, 799 F.3d at 258 (defendant violated the FTC Act where it “[d]id not use readily available security measures, such as firewalls, to limit access between and among hotels' property management systems, the Wyndham network, and the Internet.”).

6. Equifax Inappropriately Relied on Outdated and Obsolete Security Systems and Software

241. As numerous cybersecurity experts and commentators have reported since the end of the Class Period, Equifax's systems relied on outdated and obsolete

software, making the data stored on those systems vulnerable to attack. As *Forbes* reported, numerous security researchers, in post-Class Period analyses, “have found myriad old technologies running the Equifax site, many of which could be vulnerable to cyberattack.” For instance, *Forbes* reported that “Kevin Beaumont, a British security pro who’s spent 17 years helping protect businesses, found *decade-old software in use*.” According to Beaumont, “Equifax’s infrastructure is a weird mix of IBM WebSphere, Apache Struts, Java . . . *it’s like stepping back in time a decade*.” Another cybersecurity expert, Steve King, made a similar observation in a September 2017 *Security Boulevard* article, noting that Equifax’s “troubles began with a curious blend of IBM’s WebSphere, Apache Struts, and Java, which *I didn’t think anyone other than your local library branch maybe did any more*.”

242. Likewise, *Forbes* reported that “[r]esearcher Kenneth White discovered a link in the source code on the Equifax consumer sign-in page that pointed to Netscape, a web browser that was discontinued in 2008.” Some cybersecurity researchers told *Forbes* that Equifax servers were using out-of-date Java software; others, pointing to the old software running on Equifax’s systems, said that “Old IT systems could indicate lack of ‘renewal’ procedures, old and unpatched software.”

243. Researchers have further pointed out that Equifax’s reliance on old and outdated technologies exacerbated the Data Breach. As Hulme stated in an article on *Security Boulevard*, “There are many security systems that if properly installed, maintained, and used that could have detected the breach much more rapidly.”

Indeed, not only was Equifax's vulnerability scanner old and outdated, the Company was specifically warned about its reliance on old and outdated software by security researchers before the Data Breach, including in December 2016.

244. Equifax's reliance on old and outdated systems and software fall far short of security best practices, particularly given the sensitivity of the information the Company maintained. In fact, cybersecurity standards require organizations to monitor and replace outdated technologies. For example, NIST SP 800-53r4, states:

The objective of continuous monitoring plans is to determine if the complete set of planned, required, and deployed security controls within the information system, system component, or information system service continue to be effective over time based on the inevitable changes that occur.

Accordingly, cybersecurity standards require organizations to track whether protections are meaningful as time elapses. Given the fast paced change of technology, where a typical refresh cycle is 18 to 24 months, the fact Equifax was using security critical technology 10 years out of date was wholly improper.

245. Likewise, regulators have excoriated companies, including those that maintain data of far less sensitivity than Equifax does, for relying on obsolete or outdated software. The FTC has stated that "[m]aintaining and updating operating systems of computers and other devices to protect against known vulnerabilities is integral to a company's defense in depth strategy," and a company violates the FTC Act when it runs old or outdated software on systems that contain sensitive personal information. *LabMD*, 2014 WL 2142681, at *7.

7. Equifax Allowed Its “Attack Surface” to Balloon

246. During the Class Period, Equifax had thousands of servers exposed to the internet, amounting to a sprawling, unwieldy “attack surface” – providing a number of entry points for intruders – that was difficult to defend. An analysis published after the Class Period by cybersecurity consulting firm OutsideIntel showed that Equifax was managing more than 5,200 domains as of September 2017. *Motherboard* reported that Equifax’s uncontrolled “attack surface” was among the issues that a security researcher specifically raised with Equifax in December 2016.

247. Equifax’s sprawling “attack surface” during the Class Period evinced a loose control over infrastructure that was inconsistent with data security best practices. Minimizing complexity is a fundamental cybersecurity principle because the more infrastructure an organization maintains, the harder the system is to secure. The Open Web Application Security Project (OWASP) Security Principles, standards widely adopted in national and international legislation, instruct organizations to “minimize attack surface area The aim for secure development is to reduce the overall risk by reducing the attack surface area.” As security expert Claus Cramon Houmann explained, Equifax’s “huge . . . list of domains, and the web servers behind [them] and the DNS entries and so on, that in itself would require a rather well structured security operations department and a CISO in charge.” Equifax’s failure to keep security-critical aspects of its infrastructure up-to-date, such as failing to renew certificates and patch critical vulnerabilities, demonstrates

that the Company had poor control over its infrastructure. Notably, in the wake of the Data Breach, interim Equifax CEO Barros stated that one the “four critical areas of focus” in the Company’s security remediation plan was “[w]ork[ing] to streamline and simplifying our networks and application infrastructure” in order to “enhance our security posture by reducing what is known as the attack surface.”

8. Equifax Allowed Unused Data to Accumulate on Vulnerable Systems and Failed to Dispose of Unneeded Data

248. As Defendants have admitted, during the Class Period, Equifax failed to safely dispose of sensitive personal information that was no longer needed or in use. As alleged above, Smith told certain investors in private discussions after the Class Period that part of the reason the Data Breach was so extensive was because hackers had penetrated legacy databases containing decade-old information. After the Class Period, Barros testified that Equifax was only just beginning the process of “dispos[ing] of the data that [Equifax] no longer need[s].”

249. Data security best practices require companies to promptly dispose of old or unused personal information in order to avoid needlessly exposing that information to the threat of compromise. For instance, NIST standards lay out detailed requirements for the “minimization of personally identifiable information.” These standards require organizations to limit the “retention of NPPI to the minimum elements” required to accomplish the purpose for which it was collected. In order to do this, organizations must regularly review sensitive information stored in their networks to determine whether the information should be safely disposed of.

Specifically, organizations must “follow[] a schedule for regularly reviewing” sensitive data to ensure that “the NPPI continues to be necessary to accomplish the legally authorized purpose.” Equifax’s practice of allowing vast amounts of legacy data, some as much as a decade old, to be accessible via public-facing networks, violated these standards.

250. Data protection laws also mandate the prompt and safe disposal of old or unused personal information. The FTC has noted, for instance, that “[d]on’t keep what you don’t need” and “[c]lose unused ports” are “key principles” of any adequate cyberdefense system. *LabMD*, 2014 WL 2142681, at *15. Accordingly, the FTC has concluded that a company violated the FTC Act where it “maintained more data than [it] required to conduct its business,” and thus “needlessly increased the scope of potential harm resulting from a network compromise.” *Id.*

9. Equifax Failed to Restrict Access to Sensitive Data

251. Equifax failed to limit access to sensitive personal information to those employees whose job responsibilities required such access. Instead, Equifax employees had open access to personal information indiscriminately. As Steve VanWieren, Equifax’s Vice President of Data Quality who left the Company in January 2012 after almost 15 years, stated after the Class Period, “it bothered me how much access *just about any employee had to the personally identifiable attributes*. I would see printed credit files sitting near shredders, and I would hear people speaking about specific cases, speaking aloud consumer’s personally

identifiable information.” As the Warren Report explained, this improper practice persisted during the Class Period. The Warren Report concluded that Equifax, “did not adopt adequately strict security measures to properly restrict user access to sensitive data.” Indeed, in an “urgent email and spreadsheet” inadvertently emailed outside the Company and obtained by the *New York Times*, Company personnel “warned of *‘inappropriate access’ across several company systems and a ‘lack of adequate review of operating system and database credentials.’*”

252. Equifax’s improper credentialing seriously failed to meet cybersecurity best practices. The concept of “least privilege,” *i.e.*, restricting a user to only the privileges needed to do their job, is yet another fundamental security principle with which Equifax failed to comply. NIST standards devote pages describing in detail how organizations should ensure that access to information is restricted to those users that need it. Specifically, NIST standards require organizations to “audit the use of privileged information,” “prohibit non-privileged users from executing privileged functions,” and regularly review the level of security each user needs to perform their job. Likewise, the ICIT explained, “Personnel should only be assigned the least privileges necessary to fulfill their role in the organization. Privileges should be periodically reassessed to ensure that roles and needs have not changed[.]”

253. Additionally, Equifax’s failure to appropriately restrict its employees’ access to personal information contravened well-established data protection laws. The FTC has explained:

As part of a defense in depth strategy, companies that maintain sensitive information should restrict access to that data by defining roles for its employees and specifying the types of data that are needed by employees in those roles. A company that does not limit employees' access to sensitive information increases the likelihood that the data will be exposed outside of the organization, either by a malicious insider or in a compromise of the computer network.

LabMD, 2014 WL 2142681, at *17. Accordingly, a company violated the FTC Act where it “failed to use adequate measures to prevent employees from accessing Personal Information not needed to perform their jobs.” *Id.*

10. Equifax Management Failed to Foster a Strong Security Culture and Ensure Adequate Training of Security Personnel

254. Equifax failed to set a “tone at the top” that promoted data security within the Company and failed to ensure that employees responsible for data security were adequately trained and qualified. As former employees who worked in Equifax’s IT department explained to *Motherboard*, data security was not a priority at Equifax, making an incident like the Data Breach “inevitable.” One former employee told the publication, “The degree of risk [Equifax] assumes is found, by most of the IT staff who worked elsewhere, *to be preposterous.*” For example, as alleged above, a former Equifax employee told *Motherboard* that Company management refused to take seriously the conclusions of a 2016 Deloitte security audit that found multiple serious deficiencies in the Company’s infrastructure, including poor patching. Similarly, *Bloomberg* reported that Equifax management rejected the conclusions of a Mandiant investigation in early 2017, overseen by

Smith, that, like the Deloitte audit the previous year, found serious problems in the Company's security posture and recommended a broader systems review.

255. Likewise, cybersecurity experts noted that the fundamental and pervasive data security failures that contributed to the Data Breach indicated an institutional disregard for data security and a poorly trained and qualified staff. For instance, *Forbes* quoted cybersecurity expert Moehlenbruck, who explained that the Data Breach, and Equifax's improper response to it, provided strong evidence of "a lack of adequate security awareness training, which if provided at least annually, might have prevented the embarrassment of re-tweeting a phishing site link from the Equifax Twitter account not once, but 8 times!"

256. Likewise, Equifax failed to retain a qualified information security team. Most notably, neither Equifax CSO Mauldin, nor its Chief Information Officer, had adequate cybersecurity training or experience. As discussed above, Equifax was well aware that Mauldin, whose background was in music composition rather than security or even IT more generally, was not qualified to act as CSO. Accordingly, in the hours following disclosure of the Data Breach, the Company went to great lengths to erase her connection to Equifax from the internet by deleting two video interviews, removing a podcast, removing her profile from the Company's website, and changing her last name on LinkedIn to "M.," before removing her profile altogether. Equifax's efforts reflect a clear understanding that Mauldin's inadequate background was a liability.

257. As cybersecurity experts have explained, the root of Equifax's failures with respect to culture and training all flow from an inadequate "tone at the top." Moehlenbruck explained to *Forbes* that "[t]he *real problem was a very poor focus on information security at the highest levels of the company* – what we call C-level []. Training is great if it's practiced and preached throughout the organization. But evidence hints to the contrary." Likewise, ICIT's investigation of the Data Breach concluded:

In the cases of Webb and Mauldin, Equifax senior management should not have hired personnel without information security training to manage highly sensitive systems and data. Even if CVE2017-5638 [the Apache Struts vulnerability] were patched, attackers likely would have found a vector to compromise Equifax's systems because *the C-suite exhibited systemic negligence, a lack of cyber-hygiene, and a disregard for information security training and qualified personnel.*

258. Data protection best practices, as well as federal and state data protection laws, require companies like Equifax, whose principal business is the maintenance and sale of highly sensitive data, to develop a "tone at the top" that emphasizes cybersecurity, provide routine comprehensive data protection training to employees, and ensure that employees charged with protecting valuable data are qualified to do so. For example, NIST SP 800-53r4 requires that a wide range of IT and security personnel have "adequate security-related technical training specifically tailored for their assigned duties," which must address "management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures."

259. Moreover, NIST SP 800-37 emphasizes that “Senior leadership commitment to information security establishes a level of due diligence within the organization that promotes a climate for mission and business success.” NIST standards make clear that an organization’s management is responsible for establishing processes that reliably categorize data, selecting baseline security controls, implementing and assessing security controls, authorizing operation of information systems, and continuous monitoring of security controls to assess effectiveness and document changes. In particular, these standards provide that an organization’s *CEO is responsible for “establish[ing] the organizational commitment to information security and the actions required to effectively manage risk and protect the core missions and business functions* being carried out by the organization.” Among other things, the CEO is required to ensure “the organization has trained personnel sufficient to assist in complying with the information security requirements in related legislation, policies, directives, instructions, standards, and guidelines.” More broadly, the CEO “establishes appropriate accountability for information security and provides active support and oversight of monitoring and improvement for the information security program.”

260. Equifax’s institutional and organizational deficiencies fell profoundly short of the mandates of federal and state data protection laws. The FTC has made clear that the FTC Act requires an organization to “adequately train its employees to safeguard Personal Information.” *LabMD*, 2014 WL 2142681, at *5; *see also In the*

Matter of James B. Nutter & Co., A Corp., 72-3108, 2009 WL 1353454, at *1 (MSNET May 5, 2009) (Safeguards Rule rule violated by failing to implement reasonable policies and procedures for employee training, and a comprehensive written information security program); *In the Matter of Sunbelt Lending Servs., Inc.*, 139 F.T.C. 1 (2005) (Safeguards Rule violated by failure to implement reasonable employee training and appropriate oversight of the security practices of loan officers working remotely); *United States v. Vtech Electronics Ltd.*, Case No. 1:18-cv-114 (N.D. Ill. Jan. 8, 2018) (defendants violated FTC Act by failing to develop or maintain a comprehensive information security program and failing to implement reasonable guidance or training for employees regarding data security and safeguarding consumers' personal information).

11. Equifax Failed to Perform Adequate Security Reviews

261. Equifax failed to conduct adequate reviews of its systems, networks, and security. As alleged in detail above, Equifax failed to heed the calls of its cybersecurity consultants to perform comprehensive system reviews – a failure that helped allow hackers behind the Data Breach to roam Equifax's systems undetected for months. Moreover, Equifax's vulnerability scanning process was grossly deficient: scans were performed infrequently (for example, Smith admitted a scan was run only *once* between the time the Apache Struts vulnerability was published and the end of the Class Period), examined only portions of Equifax's systems, relied on outdated technology, and lacked appropriate redundancies.

262. Standard cybersecurity practice requires comprehensive security reviews at frequent intervals. As NIST standards explain, “Ongoing monitoring is a critical part of [the] risk management process.” NIST standards call for organizations to deploy continuous efficacy monitoring through automated processes where possible. Specifically, organizations should “determine if the complete set of planned, required, and deployed security controls . . . continue to be effective . . . [using] continuous monitoring plans.” Continuous monitoring systems often run every single time there is a change. NIST standards thus state that “[r]eal - time monitoring of implemented technical controls using automated tools can provide an organization with a much more dynamic view of the effectiveness of those controls and the security posture of the organization.” However, NIST makes clear that “with any comprehensive information security program, all implemented security controls, including management and operational controls, must be regularly assessed for effectiveness, even if the monitoring of such controls cannot be automated or is not easily automated.” NIST standards further provide that “the frequency of assessments should be sufficient to assure adequate security commensurate with risk.” With respect to vulnerability scanning, CIS calls for organizations to “*[r]un automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis.*” By conducting a critical security review only once between March and September 2017, despite the

sensitivity of the data stored and the knowledge that hackers were actively targeting those data, Equifax wholly failed to comply with security best practices.

263. Equifax also failed to comply with federal and state data protection laws concerning network and systems monitoring. The Safeguards Rule requires that financial institutions “regularly test[] or otherwise monitor[] the effectiveness of [their information] safeguards’ key controls, systems, and procedures.” The FTC made clear that a company fails to satisfy the Safeguards Rule where it fails to “perform a comprehensive assessment of [its] computer system.” *Fajilan*, 2011 WL 11798456, at *3; *Wyndham*, 799 F.3d 236, 258 (defendant violated the FTC Act where it failed “to conduct security investigations”).

12. Equifax Failed to Develop an Adequate Data Breach Plan

264. As Equifax’s response to the Data Breach made clear and as Smith has admitted, Equifax failed to develop an adequate data breach plan. Smith admitted in his testimony before the House Financial Services Committee, “The crisis management protocol that we have in place is a breach in general. It doesn’t specify you react differently if it’s 145 million versus 5 million.” As *Wired* reported, Equifax’s haphazard response to the Data Breach further indicates that the Company lacked an adequate data breach plan. Indeed, the Warren Report describes a number of serious deficiencies in the data breach plan Equifax produced in response to inquiries from Senator Warren’s office: (1) the plan was dated October 2014, and had not been updated in three years; (2) the plan is focused on physical security

threats, and fails to place adequate emphasis on protecting victims of cybersecurity breaches; and (3) the plan fails to provide an adequate process for informing potential victims about a data breach.

265. Cybersecurity best practices require companies, especially those like Equifax that manage an enormous volume of highly sensitive data, to develop and routinely test thorough data breach protocols. NIST standards mandate that organizations develop a data breach plan that provides for “preparation, detection and analysis, containment, eradication, and recovery.” NIST also calls for the development of a specific and comprehensive “privacy incident response plan,” which addresses “only those incidents that relate to personally identifiable information” and must describe a process for providing notice to affected individuals. In particular, NIST standards discussing the development of a notification plan point to detailed guidance on breach notification issued by the U.S. Office of Management and Budget, which, among other things requires notification plans to specify the “timeliness of the notification; source of the notification; contents of the notification” and “means of providing the notification.”

266. Likewise, federal and state data protection laws require companies to develop data breach plans that are commensurate with, among other things, the size and complexity of the organization, the nature and scope of its activities, and the sensitivity and volume of the data it maintains. The Safeguards Rule requires that financial institutions “develop, implement, and maintain a comprehensive written

information security program.” Broad or general policies are inadequate; instead, written policies and procedures must address all key risks, features, and issues. *See ACRAnet*, 2011 WL 11798455, at *2 (failure to “develop and disseminate comprehensive information security policies” violates the Safeguards Rule); *see also LabMD*, 2014 WL 2142681, at *16 (failure to develop a “sufficiently comprehensive” written security policy violates the FTC Act, and noting with approval the specific requirements NIST sets forth concerning the components of a security program).

V. ADDITIONAL ALLEGATIONS OF SCIENTER

267. Numerous allegations set forth above and summarized below give rise to the strong inference that Defendants knowingly or recklessly misled investors about Equifax’s cybersecurity, vulnerability to data breaches, compliance with data protection laws, and the Data Breach.

268. ***First***, as set forth in Section IV(E) above, Defendants received numerous warnings, both before and during the Class Period, that Equifax’s cybersecurity was inadequate to protect the sensitive personal information in its custody. For instance, as part of a March 2017 investigation that Smith was “***overseeing personally***,” and which the Company considered a “top-secret project,” Equifax’s security consulting firm, Mandiant, ***explicitly warned*** the Company that its cybersecurity was inadequate, and highlighted critical weaknesses that figured

prominently in the Data Breach: “Mandiant warned Equifax that its unpatched systems and misconfigured security policies could indicate major problems.”

269. As discussed in detail above, security consultants, auditors, and researchers provided Defendants with numerous additional warnings that the Company’s data protection measures were rife with serious weaknesses. In 2016 alone, these warnings included: (1) a Deloitte audit, which found several problems with Equifax’s cybersecurity, including a “careless approach to patching systems,” but which “[n]obody [in Equifax management] took . . . seriously”; (2) warnings from a security researcher that an immense cache of personal consumer information was easily accessible through one of its public-facing websites in unencrypted form (along with proof in the form of downloaded data sets); (3) warnings that its main websites were vulnerable to serious cross-scripting attacks; (4) warnings that researchers were able to effectively take control of many Equifax sites and servers by deploying basic attacks; (5) warnings that “[m]any [of the Company’s] servers were running outdated software”; and (6) warnings that Equifax’s “attack surface” was large and difficult to secure.

270. Moreover, both before and during the Class Period, Equifax experienced several data breaches, which revealed to Defendants vulnerabilities in the Company’s internal systems. For example, as discussed above, both Equifax’s W2Express and its TALX services were breached and employee tax information was stolen as a result of the Company’s inadequate authentication and network

monitoring protections. Defendants, including Smith, personally issued numerous soothing statements to the public that downplayed the severity of these incidents, denied that the incidents evinced deeper problems in Equifax's infrastructure, and assured the public that any security issues were minor and would be adequately addressed. Defendants, however, privately knew that these breaches were symptomatic of fundamental institutional data security failures and that those failures remained unremediated. For instance, while Equifax promised, as part of a settlement agreement, to refrain from using personal identifiers as part of its authentication measures (*e.g.*, to set passwords or usernames), it continued to do so throughout the Class Period. In addition, the numerous severe data protection problems privately reported to Equifax by researchers, consultants, and others, made clear to Defendants that the security incidents the Company experienced were the product of a fundamentally inadequate cybersecurity infrastructure, though this highly material fact remained concealed from investors.

271. Defendants also received warnings of deficiencies in its data protection measures from the government and from Equifax employees. As discussed above, Equifax received numerous clear warnings about the Apache Struts vulnerability, including emails from both U.S. CERT and from NIST, specifically flagging the vulnerability as "high" severity and urging Equifax to install the available patch. Likewise, Equifax employees warned Company management that Equifax's cybersecurity was inadequate, but, as former employees who "worked in the security

team or alongside it” explained to *Motherboard*, data security was not a priority for Equifax management, making a significant data breach “inevitable.” When, for example, Equifax employees attempted to raise the findings of Deloitte’s 2016 audit, they found that “[n]obody [in Equifax management] took [it] seriously.” Additionally, Equifax employees widely distributed an “urgent email and spreadsheet” inside the Company, which the *New York Times* reported, “warned of ‘inappropriate access’ across several company systems and a ‘lack of adequate review of operating system and database credentials.’”

272. **Second**, Defendants have admitted that they were well aware of the Data Breach by late July 2017, yet failed to disclose the breach and continued to make false statements touting Equifax’s cybersecurity for another month and a half before finally disclosing it on September 7, 2017. As alleged in detail above, Equifax has admitted that it discovered hackers had gained “unauthorized access” and “criminal access” to its networks on Saturday July 29, 2017, and that this access was extensive. Defendants have further admitted that the very next day, Mauldin, Equifax’s then-CSO, contacted John Kelly, the Company’s Chief Legal Officer, to inform him about the Data Breach. Mauldin told U.S. Senate staff that she sampled data suspected to have been compromised in the Data Breach, found that it contained sensitive personal information, and related this finding to Kelley that same week. By Sunday night, the most senior technology and security executives at Equifax were all aware of the Data Breach.

273. On July 31, 2017, news of the Data Breach was escalated to Smith, consistent with Equifax policy calling for such escalation in the event the Company's security personnel determine that a data breach is "serious." By Smith's own admission, he was told on July 31, 2017 that, at a minimum, the hack involved credit "dispute documents," which likely include personal information, such as billing details. Moreover, as Mauldin told investigators, Kelly was informed that the Data Breach "might have compromised personally identifiable information" within the first week after the hackers were discovered; it is inconceivable that Kelly would fail to report this highly material fact to Smith, especially given that Kelly notified Smith about the intrusion almost immediately after first learning about it on July 30. Thus, Defendants' own admissions establish that Smith knew the Data Breach was "serious" and that it likely involved the compromise of personal information by July 31, 2017, with the unauthorized access of personal information becoming even clearer within just the following few days.

274. Defendants have also acknowledged that, on August 2, 2017, following escalation of the Data Breach to Smith, they took dramatic steps to address the attack, including notifying the FBI about the Data Breach, and hiring King & Spalding LLP and Mandiant to conduct a "comprehensive forensic review." As cybersecurity experts have noted, and as explained above, Defendants' actions in the days following July 29, 2017 demonstrate that they understood the intrusion was serious. As cybersecurity experts have also pointed out, CFO Gamble would have

almost certainly been consulted, or at least apprised of the Company's decision to take these steps, given that engaging multiple firms to perform a "comprehensive forensic review" entails significant expense. As discussed below, the fact that Gamble sold 13% of his Equifax holdings on August 1 – the day after Smith first learned of the Data Breach, and the day before King and Spalding and Mandiant were contacted for retention – bolsters the strength of the inference that the decision to retain them, which must have been made within that timeframe, was discussed with Gamble. Indeed, Smith told the House Financial Services Committee that both Gamble and Ploder (who sold 4% of his Equifax holdings on August 2) "would be involved in many of the meetings" the CEO had about the Data Breach.

275. Finally, Smith has admitted that Mandiant issued an August 11, 2017 report confirming that large amounts of consumer information had been compromised in the Data Breach, and that he was briefed about Mandiant's conclusion by no later than August 15, 2017, yet the Data Breach remained undisclosed for almost another month. Indeed, Defendants continued to tout Equifax's cybersecurity the next day, at an August 16, 2017 investor conference.

276. ***Third***, that Defendants' false and misleading statements about Equifax's cybersecurity concerned one of the most significant issues and most profound risks the Company faced during the Class Period yields a strong inference of scienter. As Equifax acknowledged in its SEC filings during the Class Period, safeguarding the consumer information in its custody was "***critical to [Equifax's]***

business operations and strategy,” and a failure to do so would have dire consequences for the Company’s business. Likewise, in announcing the Data Breach on September 7, 2017, Smith stated that the hack “strikes at *the heart of who we are and what we do,*” and in later Congressional testimony conceded that “*data security is the number one risk*” Equifax had during the Class Period. Indeed, interim Equifax CEO Barros acknowledged that Equifax’s financial success was “predicated on [the public’s] trust [in] our IT and data security capabilities.” Moreover, Defendants were well aware that Equifax had strict obligations under federal, state, and international law to implement rigorous cyber-defense systems, and made reference to these obligations in SEC filings throughout the Class Period. Accordingly, the fact that Defendants’ misstatements concerned “the number one risk” facing Equifax, a subject that was “critical” to its business, supports an inference of severe recklessness at a minimum, particularly given the egregiousness of the Company’s improper security practices, discussed below.

277. *Fourth*, that Defendants were charged with ensuring the adequacy of Equifax’s cybersecurity and received routine updates about the state of the Company’s data security posture supports an inference of scienter. As discussed above, Defendants assured investors during the Class Period that they were deeply focused on ensuring that Equifax complied with data protection laws, and “continuously monitor[ed] federal and state legislative and regulatory activities that involve credit reporting, data privacy and security to identify issues in order to

remain in compliance” with those laws. Likewise, Dodge told investors that because a data breach would be particularly harmful to Equifax’s business, “data security and how we go about ensuring that is something we spend a lot of time and effort on.” Moreover, Smith testified that he personally had “active involvement [in monitoring Equifax’s cybersecurity] with my general counsel, with the head of security, routinely throughout the year,” and that he and other members of Equifax’s Board of Directors received “deep dives” into the Company’s risks and defenses throughout the Class Period. Smith also testified that he was frequently briefed on Equifax’s data security systems: “we would have IT reviews at least quarterly and security reviews at least quarterly. And then you would augment that on an as-needed basis.” Similarly, the Company’s 2017 Proxy statement represented that ***“Our CEO and senior leadership team receive comprehensive periodic reports on the most significant risks from the director of our internal audit department . . . including cybersecurity.”*** Either Defendants possessed the detailed knowledge of Equifax’s data protection measures they claimed to have, in which case they knew their statements on those subjects were false and misleading, or they failed to engage in the rigorous monitoring of Equifax’s cyber-risks described in their statements, rendering their repeated statements on those subjects severely reckless.

278. ***Fifth***, the egregiousness of the deficiencies in Equifax’s cybersecurity practices also strongly supports an inference of scienter. As discussed in detail in Section IV(I), above, Equifax’s improper practices contravened the most basic tenets

of standard cybersecurity practice and data protection laws, notwithstanding the fact that Defendants routinely assured investors that Equifax was diligently complying with both. As cybersecurity experts have explained, and as the pronouncements of agencies responsible for enforcing data protection laws make clear, Equifax's failures were not minor, technical, or arcane, but were blatant and pervasive, and, therefore could not reasonably have escaped management's notice. Experts explained that Equifax's improper practices demonstrated "***poor security policy and a lack of due diligence*** rather than simple oversight," "a disorganized approach to security, and a naiveté about the possibility of a breach," and likened Equifax's failures to implement basic protections as akin to failing to put "locks on your front door[.]" Experts also noted that the Data Breach itself revealed "the ***truly haphazard*** nature of Equifax's operation," and that "[a] catastrophic breach of Equifax's systems was inevitable because of ***systemic organizational disregard for cybersecurity and cyber-hygiene best practices.***" As discussed above, non-public analyses and reports issued by cybersecurity firms showed that weaknesses in Equifax's security systems were readily apparent in the months before the Data Breach, including findings that "the company was behind in basic maintenance of websites and scored poorly in areas that would likely play a role in the data breach." Likewise, Representative Maloney called Equifax's failure to implement reasonable data protection measures, "***the most open-and-shut violation of the Safeguards Rule that I have ever seen in the history of this country.***" And not only were

Equifax's cybersecurity failures egregious in character and scope, the *same improper practices persisted for years on end*, even after Equifax received numerous warnings about the risks they posed, and, in some cases, even after Equifax had explicitly agreed to remediate them.

279. Cybersecurity experts also agree that the magnitude of Equifax's data protection failures and the inordinate length of time they persisted, yields a strong inference of intentional or reckless misconduct on the part of Equifax's senior management. For instance, Senator Warren's detailed investigation found that "Equifax adopted weak cybersecurity measures that failed to protect consumer data – *a symptom of what appeared to be the low priority afforded cybersecurity by company leaders.*" Likewise, cybersecurity expert Wes Moehlenbruck told *Forbes*, "*The real problem was a very poor focus on information security at the highest levels of the company* – what we call C-level." Similarly, the ICIT's investigation of the Data Breach concluded that "*the C-suite exhibited systemic negligence, a lack of cyber-hygiene, and a disregard for information security training and qualified personnel.*" As Representative Luetkemeyer stated at an October 2017 Congressional hearing, "There's a failure on the part of [Smith], your board and your senior management." Accordingly, the magnitude of the deficiencies in Equifax's cybersecurity, and the length of time those deficiencies went unaddressed, further support an inference that Defendants' repeated statements touting the Company's

cybersecurity were made either in a deliberate attempt to deceive or in reckless disregard of obvious facts.

280. *Sixth*, the circumstances surrounding the sudden departure of high-ranking Equifax officers, just as the truth about Equifax's cybersecurity was emerging in the wake of the Data Breach, gives rise to a strong inference of scienter. As alleged above, on September 15, 2017, both Mauldin and Webb "retired" from Equifax effective immediately. Mauldin's departure followed significant efforts by the Company to erase her connection to Equifax, and her public statements on the Company's behalf, from the internet, including by deleting interviews, bios, and even her LinkedIn page. When asked at a Congressional hearing why Mauldin and Webb were permitted to "retire" rather than face termination, Smith made no effort to defend their performance. Smith instead testified that both senior executives were effectively fired, and that the distinction between retirement and termination was, in this case, mere "semantics."

281. On September 26, 2017, less than two weeks after Mauldin's and Webb's departure, Equifax announced Smith's retirement, without severance, effective immediately. As discussed above, the Board took the unusual step of announcing that it had the power to retroactively classify Smith as having been fired for cause, allowing the Company to claw back Smith's compensation. Notably, as discussed above, Smith's employment agreement restricts "cause" to intentional or reckless misconduct, including Smith's failure to do his job in a "willful and

continued” fashion. That the Board took the extraordinary step of publicly announcing the possibility that Smith’s conduct might satisfy the criteria for termination for “cause” further bolsters the inference of scienter.

282. The circumstances surrounding these sudden departures demonstrate that Equifax’s Board of Directors understood the Company was not simply the victim of unavoidable crime, and that the improper practices that led to the breach were not isolated or anomalous lapses in an otherwise sound data protection regime. Instead, the circumstances surrounding the serial departure of senior executives yield a strong inference that at the highest levels of the Company, there were profound failures in the Companies data protection practices that were the result of reckless or intentional misconduct.

283. *Seventh*, suspicious stock sales by Defendants Gamble and Ploder further support an inference of scienter. During the Class Period, Gamble sold approximately 33% of his holdings in Equifax stock. As discussed above, Gamble sold 13% of his Equifax holdings (nearly a third of his intra-Class Period sales) in a single transaction on August 1, 2017 – the day after Smith was informed about the Data Breach and the day before the Company retained teams of lawyers and security professionals to conduct a “comprehensive forensic review” of the attack. Notably, during the eighteen months preceding the start of the eighteen-month Class Period (the “Control Period”), Gamble did not sell a single share of Equifax stock. Additionally, Gamble made no open market purchases of Equifax stock during the

Class Period. Similarly, Defendant Ploder sold approximately 16% of his holdings in Equifax stock during the Class Period, and 4% of his holdings (more than 20% of his intra-Class Period sales) in a single transaction on August 2, 2017. Like Gamble, Ploder did not sell a single share of Equifax stock during the Control Period, and made no open market purchases of Equifax stock during the Class Period.

284. Defendants' suspicious stock sales, including the sales occurring just days after the Data Breach was discovered, bolsters the inference of scienter. As Senator Scott told Smith at a Congressional hearing

All those folks [investors] bore the burden of a \$6.4 billion drop in valuation. At the same time that the General Counsel who didn't know, the CEO didn't know, so all the folks in the executive suite had no clue but *they were the luckiest investors on August the 1st.*

* * *

What you all want us to believe is that the three luckiest investors who sold their stock, did so without any knowledge that that suspicious activity may be bigger and more powerful than any other suspicious activity, perhaps in the history of the company. *I find that hard to believe.*

Likewise, information security expert Adrian Sanabria explained in an article on *Savage Security Blog*:

Gamble wants us to believe that all this went down without his knowledge or approval on the sudden emergency spending? That his sudden sale of nearly \$1m worth of stock was coincidence? Equifax was first aware of the incident on a Saturday. These three [executives, including Gamble and Ploder] sold their stock the following Tuesday and Wednesday. I can guarantee you that practically the only thing that

was talked about on Monday, July 31st, was this incident. I don't buy it for a second, and neither should you.

VI. DEFENDANTS' MATERIALLY FALSE AND MISLEADING STATEMENTS

285. During the Class Period, Defendants made a host of materially false and misleading statements and omissions, which were disseminated to investors through the Company's website, during conference calls and investor presentations, and in the Company's SEC filings and press releases. Defendants' false and misleading statements and omissions generally fall into three categories: (1) false and misleading statements and omissions touting the security of Equifax's data systems and the Company's efforts to protect consumer information; (2) false and misleading statements and omissions assuring investors that Equifax's cybersecurity complied with applicable data protection laws and industry practices; and (3) false and misleading statements concerning the Company's internal controls.

A. Defendants' Materially False and Misleading Statements Concerning Equifax's Cybersecurity and the Company's Efforts to Protect Consumer Information

1. False and Misleading Statements Published on the Equifax Website

286. Throughout the Class Period, Defendants made public statements on Equifax's website that the Company protected the "privacy and confidentiality" of consumer and business information in its custody and touted the Company's commitment to strong cybersecurity:

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

287. These statements were materially false and misleading when made. It was misleading for Defendants to tout Equifax's reputation for "protect[ing] the privacy and confidentiality of personal information about consumers," to state that Equifax "protect[ed] the sensitive information [it had] about businesses," and that "[s]afeguarding the privacy and security of information . . . is a top priority" for the Company, when, in truth, Equifax's cybersecurity and data protection measures were inadequate to secure the sensitive data in Equifax's custody. In truth, and unbeknownst to investors, Equifax failed to implement basic data protection tools and procedures, including failing to implement an adequate patch management process sufficient to shield the Company from known vulnerabilities, failing to encrypt sensitive consumer data, failing to implement adequate authentication measures to prevent unauthorized access to sensitive data, and housing sensitive data on public-facing web servers easily accessible by intruders.

288. In addition, the above statements were materially false and misleading because Defendants knew or were reckless in failing to know, but failed to disclose, that hackers had penetrated Equifax's internal data systems and accessed sensitive personal information.

289. Throughout the Class Period, Defendants made public statements on Equifax’s website that the Company acted as a “trusted steward of information,” “employ[ed] strong data security and confidentiality standards,” and maintained “advanced security protections and redundancies”:

As a *trusted steward* of consumer and business information, Equifax *employs strong data security and confidentiality standards on the data we provide and on the access to that data*. We maintain a highly sophisticated data information network that includes *advanced security, protections and redundancies*.

290. These statements were materially false and misleading when made. It was misleading for Equifax to state that it serves as a “trusted steward” of consumer information, that it “employs strong data security and confidentiality standards on the data [it] provide[s] and on the access to that data,” and that it utilizes “a highly sophisticated data information network” and “advanced security, protections and redundancies,” when, in truth, Equifax’s cybersecurity and data protection measures were inadequate to secure the sensitive data in Equifax’s custody. In truth, and unbeknownst to investors, Equifax failed to implement basic data protection tools and procedures, including, among other things, failing to implement an adequate patch management process, failing to encrypt sensitive consumer data, failing to implement adequate authentication measures, and housing sensitive data on public-facing web servers easily accessible by intruders.

291. In addition, the above statements were materially false and misleading because Defendants knew or were reckless in failing to know, but failed to disclose,

that hackers had penetrated Equifax's internal data systems and accessed sensitive personal information.

292. Throughout the Class Period, Defendants made public statements on Equifax's website touting the Company's rigorous, comprehensive, and routine security reviews, as well as the Company's compliance with cybersecurity best practices, as evidenced by "security certifications":

The Equifax network is ***reviewed on a continual basis by external security experts who conduct intrusion testing, vulnerability assessments, on-site inspections, and policy/incident management reviews***. Equifax annually completes a SAS 70 Type II audit and receives TruSecure's accredited security certification. Additionally, Equifax conducts internal security reviews on a weekly basis.

293. These statements were materially false and misleading when made. It was misleading for Equifax to state that its network was "reviewed on a continual basis by external security experts" and that Equifax "conducts internal security reviews on a weekly basis," when, in truth, Equifax wholly failed to perform adequate cybersecurity reviews, and, among other things: (1) Equifax ignored advice issued by those external "security experts" warning the Company about gross inadequacies in its cybersecurity; (2) Equifax failed to heed the calls of its cybersecurity consultants to perform comprehensive system reviews – a failure that helped allow hackers behind the Data Breach to roam Equifax's systems undetected for months; and (3) Equifax's vulnerability scanning process was grossly deficient, as scans were performed infrequently, examined only portions of Equifax's systems,

relied on outdated technology, and lacked appropriate redundancies. Moreover, it was misleading for Equifax to tout its security certifications as evidence that it complied with cybersecurity best practices, when, in truth, the Company utterly failed to comply with those standards, including directives issued by NIST, PCI, SANS Institute, and OWASP, as discussed above.

294. In addition, the above statements were materially false and misleading because Defendants knew or were reckless in failing to know, but failed to disclose, that hackers had penetrated Equifax's internal data systems and accessed sensitive personal information.

295. Throughout the Class Period, Equifax's website stated that the sensitive Personal Information it controlled was encrypted and secured, stating that it used a secure web standard "*to protect, secure, and encrypt confidential information* that is transmitted over the Internet from your computer's web browser to *Equifax's secure servers*. The information is decrypted only upon receipt by Equifax."

296. These statements were materially false and misleading when made. It was misleading for Defendants to state that Equifax uses a secure network "to protect, secure, and encrypt confidential information" and that Equifax utilizes "secure servers," when, in truth, Equifax's cybersecurity framework and data protection measures were inadequate to secure the sensitive data in Equifax's custody, and, in fact, Equifax failed to encrypt sensitive personal information stored in, and transmitted over, its networks. In truth, and unbeknownst to investors,

Equifax failed to implement basic data protection tools and procedures, and stored and transmitted personal information in unencrypted, plaintext form, including on public-facing servers.

297. In addition, the above statements were materially false and misleading because Defendants knew or were reckless in failing to know, but failed to disclose, that hackers had penetrated Equifax's internal data systems and accessed sensitive personal information.

298. As alleged above, Equifax provided W-2 management services offered through its Workforce Solutions segment. Throughout the Class Period, Equifax issued assurances, including through its website, that the Company took "every precaution" to "ensure" that the highly sensitive tax and employment data maintained by Workforce Solutions would be secure. Specifically, Equifax stated, "[a]s W-2 data is sensitive and subject to federal regulations, *every precaution is taken to ensure both security and accuracy.*"

299. These statements were materially false and misleading when made. It was misleading for Equifax to state that it took "every precaution" to "ensure" that the highly sensitive data in its custody was "secur[e]," when, in truth, Equifax failed to take the most *basic* precautions to ensure that the security of the data in its custody. In truth, and unbeknownst to investors, Equifax failed to implement basic data protection tools and procedures, including, among other things, failing to implement an adequate patch management process, failing to encrypt sensitive consumer data,

failing to implement adequate authentication measures, and housing sensitive data on public-facing web servers easily accessible by intruders.

300. In addition, the above statements were materially false and misleading because Defendants knew or were reckless in failing to know, but failed to disclose, that hackers had penetrated Equifax’s internal data systems and accessed sensitive personal information.

301. Throughout the Class Period, Defendants made public statements on Equifax’s website that the Company would “securely collect and aggregate” sensitive data in connection with its “Affordable Care Act Management” services, and touted Equifax’s “proven track record of handling sensitive data”:

Our award-winning technology will *securely collect and aggregate the data* necessary to manage ACA so we can handle the processes and communication between employees, the exchanges, and the IRS. [] [Y]ou’ll have peace of mind knowing you have an audit trail and *your data is protected by Equifax’s security standards and proven track record of handling sensitive data*.

302. These statements were materially false and misleading when made. It was misleading for Equifax to state that it “securely collect[s] and aggregate[s]” sensitive data and that the data it collects “is protected by Equifax’s security standards and proven track record of handling sensitive data” when, in truth, Equifax did not “securely collect and aggregate” sensitive data; the Company’s “security standards” were inadequate to secure the sensitive data in its custody; and the Company’s so-called “track record of handling sensitive data” was belied by the

gross deficiencies in its cybersecurity. In truth, and unbeknownst to investors, Equifax failed to implement basic data protection tools and procedures, including, among other things, failing to implement an adequate patch management process, failing to encrypt sensitive consumer data, failing to implement adequate authentication measures, and housing sensitive data on public-facing web servers easily accessible by intruders.

303. In addition, the above statements were materially false and misleading because Defendants knew or were reckless in failing to know, but failed to disclose, that hackers had penetrated Equifax's internal data systems and accessed sensitive personal information.

2. Equifax's SEC Filings

304. Equifax made materially false and misleading statements concerning its cybersecurity in the Company's Form 10-K filed with the SEC on February 24, 2016 for the year ended December 31, 2015 (the "2015 Form 10-K") and its Form 10-K filed with the SEC on February 22, 2017 for the year ended December 31, 2016 (the "2016 Form 10-K"). In the 2015 Form 10-K and the 2016 Form 10-K, both signed by Defendant Smith and Defendant Gamble, Equifax stated that its "long term corporate growth strategy is driven by the following imperatives," including "[s]erv[ing] as a trusted steward and advocate for our customers and consumers . . . while simultaneously *delivering security* for our services."

305. Further, in its 2015 and 2016 Forms 10-K, Defendants Equifax, Smith, and Gamble touted the “security” of the services Equifax offered as a “differentiat[ing]” feature of its products. Specifically, these Defendants stated, “We continue to invest in and develop new technology to enhance the functionality, cost-effectiveness and *security* of the services we offer and further *differentiate our products* from those offered by our competitors.”

306. In its 2015 and 2016 Forms 10-K, Equifax stated:

Despite our *substantial investment in physical and technological security measures*, employee training, contractual precautions and business continuity plans, our information technology networks and infrastructure or those of our third-party vendors and other service providers *could be vulnerable to* damage, disruptions, shutdowns, or breaches of confidential information due to criminal conduct, denial of service or other advanced persistent attacks by hackers[.]

307. The above statement was also incorporated by reference into the quarterly reports on Form 10-Q that Equifax filed with the SEC on April 28, 2016 for the quarter ended March 31, 2016, on July 28, 2016 for the quarter ended June 30, 2016, on October 27, 2016 for the quarter ended September 30, 2016 (together, the “2016 Forms 10-Q”), on April 27, 2017 for the quarter ended March 31, 2017, and on July 27, 2017 for the quarter ended June 30, 2017 (together, the “2017 Forms 10-Q”). The 2016 Forms 10-Q and 2017 Forms 10-Q, were each signed by Defendant Smith and Defendant Gamble.

308. These statements were materially false and misleading when made. It was misleading for Defendants Equifax, Smith, and Gamble to tout Equifax’s role

“as a trusted steward ... delivering security,” stating that Equifax uses “security” to “differentiate” its products, and its “substantial investment in physical and technological security measures,” when in truth, Equifax failed to devote adequate resources and attention to securing consumer information, and failed to take fundamental steps to establish adequate cybersecurity. In truth, and unbeknownst to investors, Equifax failed to implement basic data protection tools and procedures, including, among other things, failing to implement an adequate patch management process, failing to encrypt sensitive consumer data, failing to implement adequate authentication measures, and housing sensitive data on public-facing web servers easily accessible by intruders. Moreover, it was additionally misleading for Defendants Equifax, Smith, and Gamble to state only that Equifax “*could* be vulnerable” to a data breach when, in fact, Equifax *was* highly vulnerable to such an attack, as, in fact, Defendants had been warned on numerous occasions both before and during the Class Period.

309. In Equifax’s 2015 Form 10-K and 2016 Form 10-K, Equifax stated in its risk disclosures: “We are not aware of any material breach of our data, properties, networks or systems.” Equifax incorporated this language into its 2017 Forms 10-Q, including its Form 10-Q filed on April 27, 2017 and July 27, 2017, in which Equifax stated that “[t]here have been no material changes with respect to the risk factors disclosed in our 2016 Form 10-K.”

310. The statement quoted in ¶309, and as incorporated into Equifax’s April 27, 2017 and July 27, 2017 Forms 10-Q, was materially false and misleading when made. It was misleading for Equifax to state that it was “not aware of any material breach of our data, properties, networks or systems” when Defendants knew, or were reckless in not knowing, but failed to disclose, that hackers had already penetrated Equifax’s internal data systems and accessed sensitive personal information.

311. Also in Equifax’s Forms 10-K, 2016 Forms 10-Q and 2017 Form 10-Q, Equifax stated that it maintains “secured” databases: “We develop, maintain, and enhance *secured proprietary information databases* through the compilation of consumer specific data[.]”

312. This statement was materially false and misleading when made. It was misleading for Defendants Equifax, Smith, and Gamble to state that Equifax maintains “secured proprietary information databases” when, in truth, Equifax’s cybersecurity and data protection measures were inadequate to secure the sensitive data in Equifax’s custody. In truth, and unbeknownst to investors, Equifax failed to implement basic data protection tools and procedures, including, among other things, failing to implement an adequate patch management process, failing to encrypt sensitive consumer data, failing to implement adequate authentication measures, and housing sensitive data on public-facing web servers easily accessible by intruders.

313. Equifax's SEC filings also failed to disclose material information required to be disclosed by Item 303 of Regulation S-K (17 C.F.R. §229.303), which requires the disclosure of commitments, demands, events, trends, or uncertainties reasonably likely to affect the registrant's liquidity as one of the key items requiring comprehensive disclosure. Specifically, Item 303 requires the disclosure of "any known trends or any known demands, commitments, events or uncertainties that will result in or that are reasonably likely to result in the registrant's liquidity increasing or decreasing in any material way." As the SEC explained in guidance issued on February 26, 2018, "the risks of potential cybersecurity incidents" are among the "events and uncertainties" with respect to which Item 303 contemplates disclosure.

314. Item 303's obligations required Equifax to disclose that its data protection measures were inadequate to secure the sensitive data in Equifax's custody, and that additional changes to its cybersecurity were needed to prevent a significant data breach.

3. Equifax Investor Conferences and Presentations

315. Throughout the Class Period, Equifax made a number of investor presentations and participated in industry conferences during which Defendants made materially false and misleading statements concerning Equifax's implementation of data security measures.

a. Investor Presentations

316. In presentations to investors dated September 27, 2016, November 15, 2016, December 5, 2016, February 14, 2017, March 1, 2017, May 2, 2017, June 1, 2017, and August 16, 2017, Equifax touted its “Role as a *Trusted Steward is a Key Execution Enabler*,” and that in this “role” Defendants made “*continued investments to address critical data security* throughout the company[.]”

317. These statements were materially false and misleading when made. It was misleading to state that its “role as a trusted steward is a key execution enabler” and that Equifax made “continued investments to address critical data security,” when, in truth, Equifax failed to take basic steps to act as a “trusted steward of information,” failed to devote adequate resources and attention to securing consumer information, and failed to implement adequate cybersecurity and data protection measures. In truth, and unbeknownst to investors, Equifax failed to implement basic data protection tools and procedures, including, among other things, failing to implement an adequate patch management process, failing to encrypt sensitive consumer data, failing to implement adequate authentication measures, and housing sensitive data on public-facing web servers easily accessible by intruders.

318. Defendants’ statements that Equifax’s “role as a trusted steward is a key execution enabler” and that the Company made “continued investments to address critical data security” in Equifax’s May 2, 2017, June 1, 2017, and August 16, 2017 investor presentations are additionally materially false and misleading because Defendants knew or were reckless in failing to know, but failed to disclose,

that hackers had penetrated Equifax's internal data systems and accessed sensitive personal information of 143 million people in the U.S.

319. In a presentation to investors on August 2, 2016, Equifax stated that one of the “*core strengths*” of its the Workforce Solutions segment of the Company was Equifax's service as a “steward for customers,” including the Company's “unwavering commitment to the security of [its] platform.”

320. This statement was materially false and misleading when made. It was misleading for Defendants to state that Equifax served as a “trusted steward for customers,” cite that supposed service as a “core strength” of one of its most important business segments, and tout Equifax's “[u]nwavering commitment to the security of [its] platform,” when in truth, Equifax failed to devote adequate resources and attention to securing consumer information, and failed to take fundamental steps to establish adequate cybersecurity. In truth, and unbeknownst to investors, Equifax failed to implement basic data protection tools and procedures, including, among other things, failing to implement an adequate patch management process, failing to encrypt sensitive consumer data, failing to implement adequate authentication measures, and housing sensitive data on public-facing web servers easily accessible.

321. On August 30, 2016, Equifax participated in a conference hosted by Barclays to discuss Equifax's global marketing initiatives (the “Global Marketing Conference”). In the presentation used at the Global Marketing Conference, Equifax

stated that its “corporate imperative” is to “serve as a trusted steward and advocate for our customers and consumers.”

322. This statement was materially false and misleading when made. It was misleading for Defendants to state that Equifax’s corporate imperative is to “serve as a trusted steward” when, in truth, Equifax’s cybersecurity and data protection measures were inadequate to secure the sensitive data in Equifax’s custody. In truth, and unbeknownst to investors, Equifax failed to implement basic data protection tools and procedures, including, among other things, failing to implement an adequate patch management process, failing to encrypt sensitive consumer data, failing to implement adequate authentication measures, and housing sensitive data on public-facing web servers easily accessible by intruders.

b. Investor Conferences

323. On May 18, 2016, Smith attended the Barclays Americas investor conference on behalf of Equifax. During the Barclays conference, an analyst addressed the data security risk faced by the Company, asking specifically:

[T]here’s macro risk, sort of out of your control. The other two that come up, obviously, are data security and regulation. So maybe we can start with data security. [H]ow do you guys make sure the data doesn’t bleed, and I guess you have a little bit of news with the W2 issues . . . is that an issue? How should we think about that?

In response to the analyst’s question about how Equifax “make[s] sure the data doesn’t bleed,” Defendant Smith told investors:

Data security is obviously for almost anyone, any business you're in, *a top of mind. We have a world class team, we [] never take for granted our need to continue to innovate around data security.* I think *we are in a very good position* now, but you can never become complacent as it relates to security, because a lot of people with a lot of time on their hands trying to crack that database. But all in all, we have come so far in ten years, as has the entire world, on data security. But never take it for granted. But feel like *we're in really good shape.*

324. These statements were materially false and misleading when made. It was misleading for Defendant Smith to state that “data security is . . . top of mind,” Equifax “never take[s] for granted our need” to implement rigorous cybersecurity, and the Company is “in a very good position” and “in really good shape” when, in truth, Equifax failed to devote adequate resources and attention to securing consumer information, and its cybersecurity and data protection measures were inadequate to secure the sensitive data in the Company’s custody. In truth, and unbeknownst to investors, Equifax failed to implement basic data protection tools and procedures, including, among other things, failing to implement an adequate patch management, failing to encrypt sensitive consumer data, failing to implement adequate authentication measures, and housing sensitive data on public-facing web servers easily accessible by intruders.

325. With respect to the analyst’s question about the W2Express hack (discussed above), Smith responded:

[T]hat was not [] data security. That was a customer who . . . [was] buying a particular product, it was a product with an EWS, and they [] had a very simple passcode and we recommended they change the passcode from a simple passcode to a complicated passcode, and to

reset it, and they opted not to do that, so it was within their four walls. It had nothing to do with us, so that makes that understood.

326. These statements were materially false and misleading when made. It was misleading for Defendant Smith to state that the W2Express hack was “not [a] data security” issue” and that it “had nothing to do with” Equifax, when, in fact, Equifax’s failure to implement adequate authentication, monitoring, and other cybersecurity measures contributed directly to the breach (as explained above). Moreover, Smith’s statements assuring investors that the W2Express breach did not impugn Equifax’s cybersecurity were misleading because they failed to disclose that the Company’s data protection measures were inadequate to secure the sensitive data in Equifax’s custody. In truth, and unbeknownst to investors, Equifax failed to implement basic data protection tools and procedures, including, among other things, failing to implement an adequate patch management process, failing to encrypt sensitive consumer data, failing to implement adequate authentication measures, and housing sensitive data on public-facing web servers easily accessible by intruders.

327. On August 2, 2016, Defendant Ploder participated in an investor conference hosted by Stephens securities analysts. During that conference, Ploder touted Equifax’s Affordable Care Act Management system and the support that the Company provided to the government under that program and its unemployment services. Ploder described Equifax as a “trusted steward,” stating specifically:

[T]hose two areas have put us in a situation of *being a trusted steward of their information and advocate for the human resources*

organizations and their employees. That level of trust and services and innovation, leading from the front, has allowed us to develop something called the Work Number which is a database that has information associated with income and employment of those employees of these large corporations and mid-sized corporations.

328. At that same conference, Ploder further assured investors that Equifax acted as a “trusted steward” of information, promoting growth in the Company’s verification business:

Workforce Solutions is a unit that provides services to the human resources departments of corporations. To help them comply, we manage, along with them, their payroll information. ***That trusted steward of their information for them, to give us their income and employment records,*** that in turn then we have an ecosystem of verifiers, government, the same HR organizations and also commercial entities such as financial institutions verifying income and employment information in complete alignment with USIS, and that is the model that we have; human resources, income and employment database and verifications.

329. These statements were materially false and misleading when made. It was misleading for Defendants to tout Equifax’s position as a “trusted steward” for the government and of sensitive data when, in truth, Equifax’s cybersecurity and data protection measures were inadequate to secure the sensitive data in Equifax’s custody. In truth, and unbeknownst to investors, Equifax failed to implement basic data protection tools and procedures, including, among other things, failing to implement an adequate patch management process, failing to encrypt sensitive consumer data, failing to implement adequate authentication measures, and housing sensitive data on public-facing web servers easily accessible by intruders.

330. On November 30, 2016, Equifax participated in an investor conference hosted by Cowen & Company analysts. At that conference, Dodge assured investors that, given the importance of data security to Equifax, it was something the Company “spend[s] a lot of time and effort on”:

If a company has a data breach, like a Home Depot or whatever, they can sell hammers, nails, wood, whatever and generate revenue. We have a data breach, we’re not in too good a shape out of that, right? ***So data security and how we go about ensuring that is something we spend a lot of time and effort on.***

331. This statement was materially false and misleading when made. Far from “spend[ing] a lot of time and effort on” data security, Equifax failed to take even the most basic steps to ensure that the Company’s cybersecurity and data protection measures were adequate to secure the sensitive data in Equifax’s custody. In truth, and unbeknownst to investors, Equifax failed to implement fundamental data protection tools and procedures, including, among other things, failing to implement an adequate patch management process, failing to encrypt sensitive consumer data, failing to implement adequate authentication measures, and housing sensitive data on public-facing web servers easily accessible by intruders.

332. On June 7, 2017, Defendants participated in a Stephens’ investor conference. At the investor conference, Gamble told investors that Equifax’s Workforce Solutions business served as an exchange to allow employers to verify that outside parties seeking access to data had a right to obtain it. In his comments

Defendant Gamble emphasized that the underlying purpose of this entire business line was to ensure the security of the underlying employee PI:

[T]o understand that business more clearly, that exchange [the Workforce Solutions platform] was formed to solve a problem that large employers had, which is around ensuring that the parties that were contacting them to verify the employment of individuals and their employee, when they were trying to get a mortgage or an auto loan, that when the person contacted them to say that John Gamble work there, that it's the requirement of the employer to ensure that the person contacting them actually is from a mortgage company, for example, and actually, that you have actually applied for a mortgage because the information we have can only be shared if you -- effectively you as an individual have asked for something from the counterparty. ***So the income exchange provides that level -- provides a secure verification network where the contributors, as an employer contributes information into our exchange, we make sure that the people accessing that information have a right to see it.***

333. This statement was materially false and misleading when made. It was misleading for Defendants to tout the security of Equifax's Workforce Solutions "income exchange" and state that the program "provides a secure verification network" while failing to disclose that the Company had failed to take adequate steps to protect against a data breach, which they knew would erode, if not entirely eradicate, the value of Equifax's identity and fraud products and would jeopardize the data assets they were leveraging. Moreover, it was misleading for Defendants to state that Equifax Workforce Solutions maintained a "secure" employment verification database, and that only those with "a right to see" the sensitive data maintained on that database would be able to do so when, in truth, Equifax's

cybersecurity and data protection measures were inadequate to secure the sensitive data in Equifax's custody. In truth, and unbeknownst to investors, Equifax failed to implement basic data protection tools and procedures, including, among other things, failing to implement an adequate patch management process, failing to encrypt sensitive consumer data, failing to implement adequate authentication measures, and housing sensitive data on public-facing web servers easily accessible by intruders.

334. On August 17, 2017, Defendant Smith spoke at the Terry College of Business at the University of Georgia. The speech was uploaded to YouTube.com on August 22, 2017. During Smith's speech, an audience member asked a question regarding "data fraud," specifically: "Data fraud must be a great concern of yours and everybody in the company. How do you prepare for that and how do you coordinate with other companies and other government organizations to cut down on fraud?" Smith responded that "when you have the size database we have, it's very attractive for others to try to get into our database, so it is a *huge priority* for us as you might guess. [] [Data fraud] is my number one worry, obviously."

335. Smith's statement was materially false and misleading when made. It was misleading for Smith to state that data security was a "huge priority" for Equifax and his "number one worry" when Equifax failed to take even the most basic steps to ensure that the Company's cybersecurity and data protection measures were adequate to secure the sensitive data in Equifax's custody. In truth, and

unbeknownst to investors, Equifax failed to implement fundamental data protection tools and procedures, including, among other things, failing to implement an adequate patch management process, failing to encrypt sensitive consumer data, failing to implement adequate authentication measures, and housing sensitive data on public-facing web servers easily accessible by intruders. These statements were additionally false and misleading because Defendants, including Smith personally, have admitted that they knew prior to the date of these statements but had failed to disclose, that hackers had penetrated Equifax's internal data systems and accessed sensitive personal information.

B. Defendants' Materially False and Misleading Statements Concerning Equifax's Compliance with Data Protection Laws, Regulations, and Industry Best Practices

1. False and Misleading Statements Published on the Equifax Website

336. Throughout the Class Period, Equifax stated on its website that "Equifax takes great care to *ensure that we use and process personal data in ways that comply with applicable regulations and respects individual privacy.*"

337. These statements were materially false and misleading when made. It was misleading for Defendants to state that Equifax "takes great care to ensure that we use and process personal data in ways that comply with applicable regulations and respects individual privacy," when, in truth, Equifax's cybersecurity utterly failed to comply with data protection laws and regulations, as discussed above.

Among other things, Equifax's cybersecurity practices ran afoul of the Safeguards Rule, the FTC Act, and numerous state and foreign data protection laws. Moreover, Defendants' statements that Equifax "use[d] and process[ed] personal data in ways that . . . respect[] individual privacy" was additionally false and misleading because, in truth, Equifax failed to implement data protection tools and procedures adequate to protect such data, as discussed above.

338. The above statements were also materially false and misleading because Defendants knew or were reckless in failing to know, but failed to disclose, that hackers had penetrated Equifax's internal data systems and accessed sensitive personal information.

339. Throughout the Class Period, Equifax made public statements on its website that the Company employed a "variety" of data protection measures that kept sensitive information secure, and that Equifax's data protection infrastructure complied with cybersecurity industry best practices "at all times." Specifically, Equifax stated:

Equifax uses a variety of technical, administrative and physical ways to keep personal credit data safe when we share it. For example, we require organizations to use pre-arranged secure channels to request and receive data. ***We regularly review and update our security protocols to ensure that they continue to meet or exceed established best practices at all times.***

340. These statements were materially false and misleading when made. It was misleading for Defendants to state that Equifax "uses a variety of technical,

administrative and physical ways to keep personal credit data safe,” and that Equifax “regularly review[s] and update[s] our security protocols to ensure that they continue to meet or exceed established best practices at all times,” when, in truth, Equifax’s cybersecurity utterly failed to comply with data protection best practices, including standards issued by NIST, PCI, SANS Institute, and OWASP, as discussed above. Moreover, Defendants’ statement that Equifax “uses a variety of technical, administrative and physical ways to keep personal credit data safe,” was additionally false and misleading because the “technical, administrative and physical” measures Equifax employed were wholly inadequate to “keep personal credit data safe.”

341. In addition, these statements were materially false and misleading because Defendants knew or were reckless in failing to know, but failed to disclose, that hackers had penetrated Equifax’s internal data systems and accessed sensitive personal information.

2. Equifax’s SEC Filings

342. In Equifax’s Forms 10-K, the Company acknowledged:

We are subject to a number of U.S. federal, state, local and foreign laws and regulations that involve matters central to our business. These laws and regulations may involve privacy [and] data protection. . . . In particular, we are subject to federal, state and foreign laws regarding the collection, protection, dissemination and use of non-public personal information we have in our possession to consumer financial protection.

Equifax stated in its Forms 10-K that the “security measures” the Company “employ[s] to safeguard the personal data of consumers could . . . be subject to the

FTC Act” and recognized further that any “failure to safeguard data adequately may subject [Equifax] to regulatory scrutiny or enforcement action.” The Company also represented that it was subject to provisions of the GLBA, including the GLBA Safeguards Rule and other “rules relating to the use or disclosure of the underlying data and rules relating to the physical, administrative and technological protection of non-public personal financial information.” In addition to these requirements, Equifax stated that it was subject to state data security breach laws, among other things, many of which “require additional data protection measures which exceed” those imposed by federal law. After enumerating the various federal and state data protection laws and regulations to which it subject, Equifax assured investors that it was in compliance with them:

We continuously monitor federal and state legislative and regulatory activities that involve credit reporting, data privacy and security to identify issues *in order to remain in compliance with all applicable laws and regulations.*

343. The above statements were materially false and misleading. It was misleading for Defendants to state that Equifax “remain[s] in compliance with all applicable laws and regulations” when, in truth, Equifax’s cybersecurity utterly failed to comply with data protection laws and regulations, as discussed above. Among other things, Equifax’s cybersecurity practices ran afoul of the Safeguards Rule, the FTC Act, numerous state and foreign data protection laws and industry – accepted best practices. Indeed, Representative Maloney called Equifax’s failure to

implement reasonable data protection measures, “the most open-and-shut violation of the Safeguards Rule that I have ever seen in the history of this country.”

344. Equifax further stated in its “risk factors” in its 2015 Form 10-K and 2016 Form 10-K that the Company was “subject to a number of U.S. and state and foreign laws and regulations relating to consumer privacy, data and financial protection,” and that it was “devot[ing] substantial compliance, legal and operational business resources to *facilitate compliance with applicable regulations and requirements.*” This statement was incorporated into Equifax’s 2016 Forms 10-Q and 2017 Forms 10-Q.

345. This statement was materially false and misleading. It was misleading for Defendants to state that Equifax “facilitate[s] compliance with applicable regulations and requirements” when, in truth, Equifax’s cybersecurity utterly failed to take basic steps to comply with data protection laws and regulations, as discussed above. Among other things, Equifax’s cybersecurity practices ran afoul of the Safeguards Rule, the FTC Act, numerous state and foreign data protection laws and industry-standard best-practices.

346. On March 24, 2017, Equifax filed a proxy statement on Schedule 14A with the SEC. In its proxy, Equifax assured investors that it implemented a “rigorous enterprise risk management program” that specifically targeted the Company’s cybersecurity risks and involved Defendant Smith and the “senior leadership team” receiving “comprehensive periodic reports”:

We have a rigorous enterprise risk management program targeting controls over operational, financial, legal/regulatory compliance, reputational, technology, privacy, ***data security***, strategic and other risks that could adversely affect our business.

* * *

Our CEO and senior leadership team receive comprehensive periodic reports on the most significant risks from the director of our internal audit department. In addition, our director of internal audit reports to the Audit Committee on a quarterly basis and reports annually to the full Board, as described below under “Board Risk Oversight.”

* * *

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.***

347. These statements were materially false and misleading when made. It was misleading for Defendants to state that Equifax implemented a “rigorous” risk management program targeting the Company’s “controls over . . . data security” and “legal and regulatory compliance,” when, in truth, Equifax failed to take basic steps to implement adequate cybersecurity controls, failed to adequately monitor and review the effectiveness of the Company’s data protection measures (despite calls from Equifax consultants to perform comprehensive reviews), failed to implement adequate vulnerability scanning processes, failed to develop an adequate data breach program, and failed to adequately train personnel. Moreover, Defendants statements touting Equifax’s risk management program targeting “legal and regulatory

compliance” and “regulatory and other compliance risks” were misleading because they failed to disclose that Equifax utterly failed to comply with data protection laws and regulations, as discussed above. Among other things, Equifax’s cybersecurity practices ran afoul of the Safeguards Rule, the FTC Act, and numerous state and foreign data protection laws. Additionally, in Equifax’s 2018 proxy statement filed on Schedule 14A with the SEC on April 2, 2018, Equifax admitted that in response to the Data Breach and “[i]n an effort to strengthen our enterprise risk management program, we are in the process of implementing a new ERM framework,” further demonstrating the falsity of the above statements.

348. These statements were also materially false and misleading because Defendants knew or were reckless in failing to know, but failed to disclose, that hackers had penetrated Equifax’s internal data systems and accessed sensitive personal information.

C. Defendants’ False and Misleading Statements Concerning Equifax’s Internal Controls

349. Equifax’s Class Period 2015 and 2016 Forms 10-K represented that the Company’s internal controls would provide “reasonable assurance regarding *prevention or timely detection of unauthorized acquisition, use or disposition of our assets* that could have a material effect on the financial statements.” With respect to this aspect of Equifax’s internal controls, Defendants Equifax, Smith and Gamble represented in the Forms 10-K that “management concluded that . . . Equifax’s internal control over financial reporting was effective.”

350. In connection with Equifax's Forms 10-K and Forms 10-Q, Defendants Smith and Gamble signed certifications pursuant to the Sarbanes-Oxley Act ("SOX Certifications"). Smith and Gamble certified that Equifax's internal disclosure controls and procedures, including those cited in the foregoing paragraph, were effective. Specifically, Smith and Gamble certified that they:

Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared.

The SOX Certifications also said Smith and Gamble had disclosed "All significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant's ability to record, process, summarize and report financial information."

351. Equifax's SEC filings further recited Smith's and Gamble's conclusion that Equifax's internal reporting controls

(i) were appropriately designed to provide reasonable assurance of achieving their objectives and (ii) were effective and provided reasonable assurance that the information required to be disclosed by Equifax in reports filed under the Exchange Act is (a) recorded, processed, summarized and reported within the time periods specified in the SEC's rules and forms and (b) accumulated and communicated to Equifax's management, including our Chairman and Chief Executive Officer and Chief Financial Officer, as appropriate to allow timely decisions regarding required disclosure.

352. The preceding statements regarding Equifax's internal controls, and Defendant Smith's and Defendant Gamble's SOX Certifications were materially false and misleading when made. As the SEC's February 26, 2018 guidance explains, the adequacy of an issuer's internal reporting controls depends on the effectiveness of its processes and procedures for ensuring that material "cybersecurity risks and incidents" are adequately disclosed. As alleged above, Equifax lacked adequate internal mechanisms for detecting breaches of its data networks and failed to design and implement an adequate data breach protocol that would facilitate prompt and materially complete disclosure of such breaches. Accordingly, Defendants' representations that its internal controls would "prevent" and "detect" unauthorized access or acquisition of the Company's vast stores of personal information were materially false and misleading and Defendant Smith's and Defendant Gamble's SOX certifications concerning Equifax's internal controls were materially false and misleading when made.

353. As alleged above, Equifax lacked adequate internal mechanisms for detecting breaches of its data networks and failed to design and implement an adequate data breach protocol that would facilitate prompt and materially complete disclosure of such breaches.

VII. LOSS CAUSATION

354. Defendants' wrongful conduct, as alleged herein, directly and proximately caused the economic loss suffered by Lead Plaintiff and the Class.

Throughout the Class Period, Equifax's stock price was artificially inflated as a result of Defendants' materially false and misleading statements and omissions concerning: (i) Equifax's data systems and the Company's efforts to protect consumer information, while failing to disclose that Equifax's cybersecurity; (2) Equifax's compliance with applicable data protection laws and industry practices; and (3) the Company's internal controls. Defendants also omitted to disclose, and made misleading statements in light of, the occurrence of the Data Breach.

355. Multiple disclosures on these topics revealed to the market on a piecemeal basis the false and misleading character of Defendants' statements and omissions. First, on September 7, 2017, after the close of trading, Defendants disclosed that Equifax had experienced a massive breach of its networks as early as May 2017. This announcement, and the information publicly reported by other sources, including those referenced above, partially revealed the truth concealed by Defendants' misstatements, as the market understood that intruders were able to gain access to Equifax's systems, access highly sensitive data, and go undiscovered for several months. These revelations partially corrected Defendants' prior misrepresentations and omissions concerning Equifax's: (a) data protection efforts and commitment to cybersecurity; (b) compliance with applicable cybersecurity standards set by law, regulation or industry standard; (c) the adequacy of the Company's internal controls; and (d) failure to timely detect and/or disclose the occurrence of the Data Breach. Accordingly, Equifax's stock price declined in

response to these revelations by a statistically significant amount when controlling for market and peer-group factors, thereby causing damage to Lead Plaintiff and other members of the Class as a portion of the artificial inflation in the Company's stock price was removed. Specifically, in trading on September 8, 2017, Equifax stock fell 14% from its September 7, 2017 closing price of \$142.72, to close at \$123.23 per share on September 8, on extremely heavy volume of nearly 17 million shares traded.

356. However, Equifax's September 7, 2017 disclosure did not reveal the full truth to investors. While Defendants made statements meant to reassure the market of their commitment to protecting consumers, investors were left in the dark as to how egregious Defendants' cybersecurity failures really were, and what these failures would mean for Equifax.

357. *Second*, from after the close of trading on Friday, September 8, 2017 through the close of trading on Monday, September 11, 2017, investors further learned of the depth and scope of Defendants' cybersecurity failures, particularly the Company's failure to have an effective and comprehensive crisis management plan in place in the event of a data breach. During that time period, it was revealed to investors that Equifax's poor cybersecurity not only allowed the Data Breach, but lacked the basic planning, management, infrastructure and tools to effectively manage their response. Despite having control over when they disclosed the Data Breach and at least five weeks from when it was purportedly discovered, Defendants

made a number of critical mistakes reflecting carelessness and lack of organization or foresight. Investors also learned prior to and during the trading day on Monday, September 11, that Congress was conducting a probe into Equifax—not just its handling of the Data Breach, but its data security more generally—indicating to the market that there were significant problems with Equifax’s legal and regulatory compliance around cybersecurity. The truth concealed by Defendants’ materially false and misleading statements and omissions was thus partially revealed through these disclosures, including those referenced above. These revelations partially corrected Defendants’ prior misrepresentations and omissions concerning Equifax’s: (a) data protection efforts and commitment to cybersecurity; (b) compliance with applicable cybersecurity standards set by law, regulation or industry standard; and (c) the adequacy of the Company’s internal controls. These additional partial revelations caused a statistically significant decline in the price of Equifax stock, when controlling for market and peer-group factors, and thus removed part of the artificial inflation in Equifax’s share price, causing damage to Lead Plaintiff and other members of the Class. Specifically, in response to the information revealed from the close of trading on September 8 through the close of trading on September 11, Equifax shares fell another 9%, from \$123.23 per share on September 8 to \$113.12 on September 11, on heavy volume of approximately 9.8 million shares traded on Monday, September 11. As before, however, these disclosures failed to reveal the full truth to investors.

358. *Third*, between the close of trading on September 12, 2017 and the close of trading on September 13, 2017, the market learned even more about Equifax's cybersecurity failures and the implications of those failures on the Company, including that investors were also then able to quantify the financial impact the Data Breach would have on the Company's TrustedID business. Smith's apology and disclosure on September 12, after the close of trading, that, to date, 11.5 million consumers had taken advantage of Equifax's free TrustedID offering, showed how severe an impact the Data Breach would have on the Company's Global Consumer segment. The truth concealed by Defendants' materially false and misleading statements and omissions was thus partially revealed through these disclosures and the information publicly reported by other sources, including those referenced above. These revelations partially corrected Defendants' prior misrepresentations and omissions concerning Equifax's: (a) data protection efforts and commitment to cybersecurity; and (b) the adequacy of the Company's internal controls. These additional partial revelations caused a statistically significant decline in the price of Equifax stock, when controlling for market and peer-group factors, and thus further removed a portion of the artificial inflation in Equifax's share price, causing damage to Lead Plaintiff and other members of the Class. Specifically, in response to the disclosures occurring between the close of trading on September 12, 2017 and the close of trading on September 13, 2017, shares of Equifax fell again, from their September 12, 2017 closing price of \$115.96 to close at \$98.99 on September 13, a

decline of 14.6% on extremely heavy volume of approximately 17.5 million shares traded. These disclosures, however, did not reveal the full truth to investors, who were still unaware of all relevant facts, including the underlying security weakness that allowed the Data Breach.

359. *Fourth*, between the close of trading on September 13, 2017 and the close of trading on September 14, 2017, the market learned how pervasive and fundamental Equifax's cybersecurity failures were, and that had it not been for these failures, the Data Breach would have been avoided. Specifically, after market close on September 13, Defendants disclosed that the underlying weakness that allowed the Data Breach was a flaw in Equifax's Apache Struts open-source software that was first publicized months earlier, in March 2017, and for which a patch was made available the very next day. The truth concealed by Defendants' materially false and misleading statements and omissions was thus partially revealed through these disclosures and the information publicly reported by other sources, including those referenced above, alerted investors to Defendants' careless approach to data security, and made clear that Equifax's deficiencies were fundamental and pervasive, that Equifax was not in compliance with applicable laws and regulations, and had inadequate internal controls. The severity of these failures was further confirmed by news that Congressional committees and a coalition of state attorneys general were conducting probes into Equifax. These revelations partially corrected Defendants' prior misrepresentations and omissions concerning Equifax's: (a) data protection

efforts and commitment to cybersecurity; (b) compliance with applicable cybersecurity standards set by law, regulation or industry standard; and (c) the adequacy of the Company's internal controls. These additional partial revelations caused a statistically significant decline in the price of Equifax stock, when controlling for market and peer-group factors, and further removed part of the artificial inflation in Equifax's share price, causing damage to Lead Plaintiff and other members of the Class. Specifically, in response to the information revealed from the close of trading on September 13 through the close of trading on September 14 shares of Equifax common stock fell again, to close on Thursday, September 14, 2017 at \$96.66, a further decline of \$2.33 per share from the September 13, 2017 closing price. Though these disclosures further informed the market of Equifax's profound cybersecurity deficiencies, they did not reveal the full truth to investors.

360. *Finally*, on September 15, 2017, Equifax's Chief Security Officer and Chief Information Officer both resigned, effective immediately. This disclosure, and the information publicly reported by other sources, including those referenced above, revealed to the market that the Company's internal cybersecurity management and infrastructure were inadequate, that its senior executives had not created proper and adequate internal controls, and that the Company had not been in compliance with applicable laws and regulations. These revelations partially corrected Defendants' prior misrepresentations and omissions concerning Equifax's: (a) data protection efforts and commitment to cybersecurity; (b) compliance with

applicable cybersecurity standards set by law, regulation or industry standard; and (c) the adequacy of the Company's internal controls. These additional revelations caused a statistically significant decline in the price of Equifax stock, when controlling for market and peer-group factors, and thus removed artificial inflation in Equifax's share price, causing damage to Lead Plaintiff and other members of the Class. Specifically, on September 15, 2017 Equifax's stock price declined by an additional \$3.68 per share, or approximately 4%, from its \$96.66 closing price on Thursday, September 14, 2017, to close at \$92.98 per share, on heavy trading volume of 16.7 million shares.

361. None of these revelations was sufficient on its own to fully remove the inflation from Equifax's stock price because each only partially revealed the risks and conditions that had been concealed from or misrepresented to investors. Moreover, as explained above, the corrective impact of the disclosures alleged herein was tempered by Defendants' continued reassuring statements and failure to fully disclose the facts of the Data Breach.

362. The decline in Equifax's stock price was a direct and proximate result of Defendants' scheme being revealed to investors and to the market. The timing and magnitude of Equifax's stock price declines negates any inference that the economic losses and damages suffered by Lead Plaintiff and the other members of the Class were caused by changed market conditions, macroeconomic factors, or even Equifax-specific facts unrelated to the Equifax Defendants' fraudulent conduct.

VIII. PRESUMPTION OF RELIANCE

363. At all relevant times, the market for Equifax's securities was efficient for the following reasons, among others:

- (a) Equifax's stock met the requirements for listing, and was listed and actively traded on the New York Stock Exchange ("NYSE"), a highly efficient market;
- (b) As a regulated issuer, Equifax filed periodic reports with the SEC and the NYSE;
- (c) Equifax shares traded regularly and with significant volume, with an average daily volume of 519,000 shares traded on the NYSE during the Class Period;
- (d) Equifax regularly communicated with public investors via established market communication mechanisms, including through regular disseminations of press releases on the national circuits of major newswire services, through the Company's website, and through other wide-ranging public disclosures, such as communications with the financial press and other similar reporting services; and
- (e) Equifax was followed by numerous securities analysts employed by major brokerage firms who wrote reports that were distributed to those brokerage firms' sales force and certain customers. Each of these reports was publicly available and entered the public market place.

364. As a result of the foregoing, the market for Equifax stock promptly digested current information regarding Equifax from all publicly available sources and reflected such information in Equifax's stock price. Under these circumstances, all purchasers of Equifax securities during the Class Period suffered similar injury through their purchase of Equifax securities at artificially inflated prices, and a presumption of reliance applies.

365. In addition, Lead Plaintiff is entitled to a presumption of reliance under *Affiliated Ute Citizens of Utah v. U.S.*, 406 U.S. 128 (1972), because the claims asserted herein are predicated in part upon material omissions of fact that Defendants had a duty to disclose.

IX. INAPPLICABILITY OF THE STATUTORY SAFE HARBOR

366. The statutory safe harbor provided for forward-looking statements under certain circumstances does not apply to any of the allegedly false statements described in this Complaint. Many of the specific statements described herein were not identified as “forward-looking” when made. To the extent that there were any forward-looking statements, there was no meaningful cautionary language identifying important factors that could cause actual results to differ materially from those in the purportedly forward-looking statements. Alternatively, to the extent that the statutory safe harbor does apply to any forward-looking statements described herein, Defendants are liable for those false forward-looking statements because at the time each was made, the particular speaker knew that the particular forward-looking statement was false or misleading, and/or that the forward-looking statement was authorized and/or approved by an executive officer of Equifax who knew that those statements were false or misleading when made.

X. CLASS ACTION ALLEGATIONS

367. Lead Plaintiff brings this action as a class action pursuant to Fed. R. Civ. P. 23(a) and 23(b)(3) on behalf of a class consisting of all those who purchased

or otherwise acquired Equifax securities between February 25, 2016 through September 15, 2017, inclusive, and who were damaged thereby (the “Class”). Excluded from the Class are Defendants, the officers and directors of Equifax at all relevant times, members of their immediate families and their legal representatives, heirs, successors or assigns, and any entity in which Defendants have or had a controlling interest.

368. The members of the Class are so numerous that joinder of all members is impracticable. Throughout the Class Period, Equifax common shares were actively traded on the NYSE. As of January 31, 2018, Equifax had approximately 120,123,872 shares of common stock outstanding. While the exact number of Class members is unknown to Lead Plaintiff at this time and can only be ascertained through appropriate discovery, Lead Plaintiff believes that there are hundreds or thousands of members of the proposed Class. Class members who purchased Equifax common shares may be identified from records maintained by Equifax or its transfer agent(s), and may be notified of this class action using a form of notice similar to that customarily used in securities class actions.

369. Lead Plaintiff’s claims are typical of Class members’ claims, as all members of the Class were similarly affected by Defendants’ wrongful conduct in violation of federal law that is complained of herein.

370. Lead Plaintiff will fairly and adequately protect Class members' interests and has retained competent counsel experienced in class actions and securities litigation.

371. Common questions of law and fact exist as to all Class members and predominate over any questions solely affecting individual Class members. Among the questions of fact and law common to the Class are:

- (a) whether the federal securities laws were violated by Defendants' acts as alleged herein;
- (b) whether statements made by Defendants to the investing public during the Class Period misrepresented material facts about Equifax's cybersecurity, the vulnerability of its information systems to unauthorized intrusions, the Company's compliance with data protection law, regulations, and best practices, and the risks associated with the Company's identity protection and verification services;
- (c) whether Defendants acted with scienter; and
- (d) to what extent the members of the Class have suffered damages, as well as the proper measure of damages.

372. A class action is superior to all other available methods for the fair and efficient adjudication of this action because joinder of all Class members is impracticable. Additionally, the damage suffered by some individual Class members may be small so that the burden and expense of individual litigation makes it impossible for such members to individually redress the wrong done to them. There will be no difficulty in the management of this action as a class action.

XI. COUNTS

COUNT I

VIOLATIONS OF SECTION 10(b) OF THE EXCHANGE ACT AND RULE 10b-5 PROMULGATED THEREUNDER (Against All Defendants)

373. Lead Plaintiff repeats and re-alleges each and every allegation set forth above as if fully set forth herein.

374. This Count is asserted on behalf of all members of the Class against Defendants Equifax, Smith, Gamble, Ploder, and Dodge for violations of Section 10(b) of the Exchange Act, 15 U.S.C. § 78j(b) and Rule 10b-5 promulgated thereunder, 17 C.F.R. § 240.10b-5.

375. During the Class Period, Defendants Smith, Gamble, Ploder and Dodge carried out a plan, scheme and course of conduct which was intended to, and throughout the Class Period, did: (i) deceive the investing public regarding Equifax's business, operations, management and the intrinsic value of Equifax securities; (ii) enabled Defendants to artificially inflate the price of Equifax securities; and (iii) caused Lead Plaintiff and other members of the Class to purchase Equifax securities at artificially inflated prices. In furtherance of this unlawful scheme, plan and course of conduct, Defendants jointly and individually took the actions set forth herein.

376. The Defendants named in this count: (i) employed devices, schemes, and artifices to defraud; (ii) made untrue statements of material facts or omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; and/or (iii) engaged in

acts, practices, and a course of business that operated as a fraud or deceit upon the purchasers of the Company's securities during the Class Period in an effort to maintain artificially high market prices for Equifax securities in violation of Section 10(b) of the Exchange Act and Rule 10b-5. The Defendants named in this count are sued as primary participants in the wrongful and illegal conduct charged herein. Defendants Smith and Gamble are also sued as controlling persons as alleged below.

377. These Defendants, individually and in concert, directly and indirectly, by the use, means or instrumentalities of interstate commerce and/or of the mails, engaged and participated in a continuous course of conduct to conceal and misrepresent adverse material information about the business, operations and financial results of Equifax as specified herein.

378. These Defendants employed devices, schemes and artifices to defraud, while in possession of, or recklessly ignoring, material adverse non-public information and engaged in acts, practices, and a course of conduct as alleged herein in an effort to assure investors of Equifax's value and performance and continued substantial growth, which included the making of, and the participation in the making of, untrue statements of material facts and omitting to state material facts necessary in order to make the statements made, not misleading, as set forth more particularly herein, and engaged in transactions, practices and a course of business which operated as a fraud and deceit upon the purchasers of Equifax securities during the Class Period.

379. Defendants are liable for the materially false and misleading statements and omissions they made during the Class Period as alleged in detail above in Section VI.

380. Defendants Smith, Gamble, Ploder, and Dodge, as the most senior officers of the Company, are liable as direct participants in the wrongs complained of herein. Through their high-ranking positions of control and authority as the most senior executive officers of the Company, each of these Defendants was able to control, and did directly control, the content of the public statements disseminated by Equifax. Defendants Smith, Gamble, Ploder, and Dodge had direct involvement in the daily business of the Company and either made personally or participated in the preparation and dissemination of the materially false and misleading statements set forth above.

381. The allegations in this Complaint establish a strong inference that Defendants Equifax, Smith, Gamble, Ploder, and Dodge acted with scienter throughout the Class Period in that they had actual knowledge of the misrepresentations and omissions of material facts set forth herein, or acted with reckless disregard for the truth in that they failed to ascertain and disclose such facts. As demonstrated by Defendants' material misstatements and omissions throughout the Class Period, if Defendants did not have actual knowledge of the misrepresentations and omissions alleged herein, they were reckless in failing to obtain such knowledge by recklessly refraining from taking those steps necessary to

discover whether their statements were false or misleading, even though such facts were available to them.

382. By virtue of the foregoing, Defendants have violated Section 10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder.

383. As a direct and proximate result of Defendants' wrongful conduct, Lead Plaintiff and the other members of the Class suffered damages in connection with their respective purchases of Equifax securities during the Class Period.

COUNT II

VIOLATIONS OF SECTION 20(a) OF THE EXCHANGE ACT (Against The Individual Defendants)

384. Lead Plaintiff repeats and re-alleges each and every allegation set forth above as if fully set forth herein.

385. This Count is asserted on behalf of all members of the Class against Defendants Smith, Gamble, Dodge and Ploder for violations of Section 20(a) of the Exchange Act, 15 U.S.C. § 78t(a).

386. By reason of their high-level positions of control and authority as the Company's most senior officers and, in the case of Defendant Smith as its Director, the Individual Defendants had the power and authority to influence and control, and did influence and control, the decision-making and activities of the Company and its employees, and to cause the Company to engage in the wrongful conduct complained of herein. The Individual Defendants were able to and did influence and control, directly and indirectly, the content and dissemination of the public

statements made by Equifax during the Class Period, thereby causing the dissemination of the false and misleading statements and omissions of material facts as alleged herein. The Executive Defendants were provided with or had unlimited access to copies of the Company's press releases, public filings and other statements alleged by Lead 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.

387. In their capacities as Equifax's most senior corporate officers, and as more fully described above, Defendants Smith, Gamble, Ploder and Dodge had direct and supervisory involvement in the day-to-day operations of the Company and, therefore, are presumed to have had the power to control or influence the particular transactions giving rise to the securities law violations as alleged herein. Defendants Smith and Gamble signed Equifax's SEC filings and Sarbanes-Oxley certifications, and were directly involved in providing false information and certifying and/or approving the false statements disseminated by Equifax during the Class Period.

388. Each of the Defendants culpably participated in the fraud alleged herein. Defendants Smith, Gamble, Ploder and Dodge each acted with scienter, as set forth more fully in Section V.

389. By virtue of their positions as controlling persons of Equifax and as a result of their own aforementioned conduct, Defendants Smith and Gamble, together

and individually, are liable pursuant to Section 20(a) of the Exchange Act, jointly and severally with, and to the same extent as the Company is liable under Section 10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder.

XII. PRAYER FOR RELIEF

WHEREFORE, Lead Plaintiff respectfully prays for judgment as follows:

- (a) Determining that this action is a proper class action maintained under Rules 23(a) and (b)(3) of the Federal Rules of Civil Procedure, certifying Lead Plaintiff as class representatives, and appointing Bernstein Litowitz Berger & Grossmann LLP as class counsel pursuant to Rule 23(g);
- (b) Declaring and determining that Defendants violated the Exchange Act by reason of the acts and omissions alleged herein;
- (c) Awarding Lead Plaintiff and the Class compensatory damages against all Defendants, jointly and severally, in an amount to be proven at trial together with prejudgment interest thereon;
- (d) Awarding Lead Plaintiff and the Class their reasonable costs and expenses incurred in this action, including but not limited to, attorney's fees and costs incurred by consulting and testifying expert witnesses; and
- (e) Granting such other and further relief as the Court deems just and proper.

XIII. JURY DEMAND

390. Lead Plaintiff demands a trial by jury of all issues so triable.

DATED: April 23, 2018

Respectfully submitted,

/s/ James A. Harrod

James A. Harrod

Abe Alexander

Brenna Nelinson

**BERNSTEIN LITOWITZ BERGER
& GROSSMANN LLP**

1251 Avenue of the Americas

New York, New York 10020

Telephone: (212) 554-1400

Facsimile: (212) 554-1444

jim.harrod@blbglaw.com

abe.alexander@blbglaw.com

brenna.nelinson@blbglaw.com

*Counsel for Lead Plaintiff Union Asset
Management Holding AG and Lead Counsel
for the Class*

H. Lamar Mixson

Georgia Bar No. 514012

Amanda Seals Bersinger

Georgia Bar No. 502720

**BONDURANT MIXSON &
ELMORE LLP**

1201 West Peachtree Street NW

Suite 3900

Atlanta, GA 30309

Telephone: (404) 881-4100


Facsimile: (404) 881-4111

mixson@bmelaw.com

bersinger@bmelaw.com

*Local Counsel for Lead Plaintiff Union Asset
Management Holding*

APPENDIX



bumblebee_equifax.jdbc.password	*****
briteline-rbc.jdbc.url	jdbc:mysql://br[REDACTED]
bumblebee_fis.jdbc.username	b[REDACTED]
bumblebee.restful-consumer.url	http://bumblebeeconsumer[REDACTED]
aws.cluster.accessKey	*****
aws.cluster.secretKey	*****
equifax.api.password.aws	ve[REDACTED]
bumblebee.jdbc.username	b[REDACTED]
elastic.host.aws	https://sear[REDACTED]
equifax.api.security.code.aws	@U2
fisApi.username	use[REDACTED]
bumblebee.fisRelay.sendMail.url	mail/v1/se[REDACTED]
equifax.api.url.aws	https://[REDACTED].equifax.com/ists/stspost
fis.capRoll.stifle.aws.bucketKey	*****
bumblebee_schedule.jdbc.password	*****
bumblebee.etl.jdbc.password	*****
elastic.index.aws	logs[REDACTED]lebee
elastic.secretKey.aws	dE[REDACTED]Ubu
bumblebee_equifax.jdbc.username	bet[REDACTED]

Figure 1. Screenshot published by Equifax hackers after the Class Period indicating that Equifax continued to leave private encryption keys on its network through September 2017.



Figure 2. Researcher's Tweet showing that the researcher notified Equifax in 2016 that the Company's main website was vulnerable to a dangerous cross-site scripting attack, but that as of September 7, 2017, this vulnerability had still not been patched.



The graphic is titled "Coordinated Disclosure Timeline" in orange text with a small orange icon to the left. It contains a table with four rows of events and their corresponding timestamps.

Vulnerability submitted via Open Bug Bounty	14 March, 2016 13:56 GMT
Generic security notifications sent to website owner	14 March, 2016 13:59 GMT
Notification sent to subscribers (without technical details)	14 March, 2016 14:17 GMT
Vulnerability details disclosed by researcher	6 June, 2016 14:15 GMT

Figure 2A. Image from researcher's Tweet in Figure 2, above, showing that the researcher notified Equifax in March 2016 that the Company's main website was vulnerable to an XSS attack.

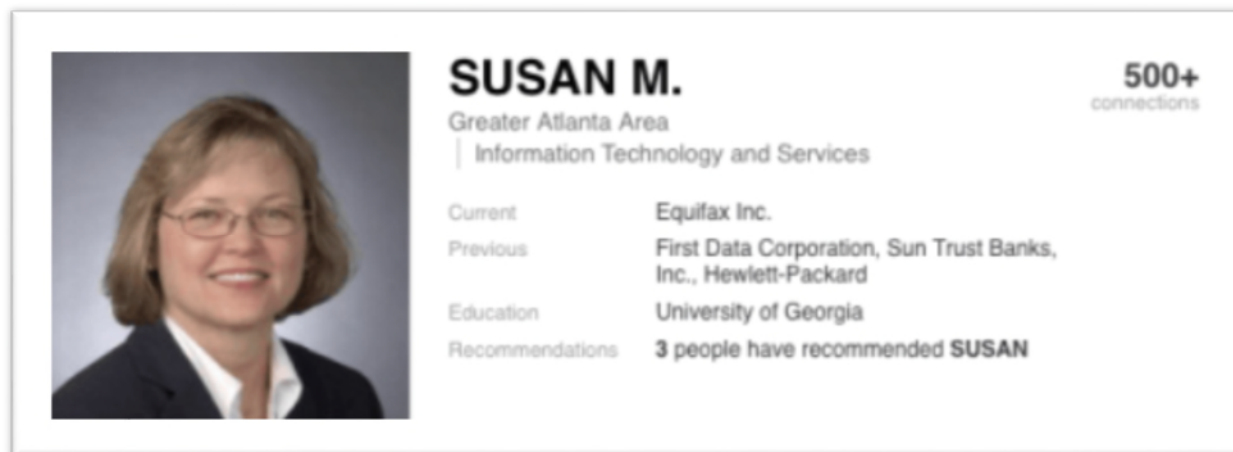


Figure 3. Image from former Equifax Chief Security Officer Susan Mauldin's LinkedIn page following the Company's announcement of the Data Breach, with all credentials removed.

CERTIFICATE OF SERVICE

I hereby certify that on this 23rd day of April, 2018, I caused a true and correct copy of the foregoing to be electronically filed with the Clerk of the Court using the CM/ECF system, which will automatically send notification of such filing and make available the same to all counsel of record.

/s/ James A. Harrod

James A. Harrod (*pro hac vice*)