UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

IN RE: EQUIFAX, INC. CUSTOMER DATA SECURITY BREACH LITIGATION	MDL Docket No. 2800 No. 1:17-md-2800-TWT
THIS DOCUMENT RELATES TO: ALL FINANCIAL INSTITUTION ACTIONS	Chief Judge Thomas W. Thrash, Jr.

FINANCIAL INSTITUTION PLAINTIFFS' [PROPOSED] SECOND AMENDED CONSOLIDATED COMPLAINT

"*[T]here's no doubt that securing data is the core value of our company. And I will [] apologize deeply to the American public for the breach that we had. We let the public down.*"

Richard Smith, Former Chief Executive Officer of Equifax Inc.
Nov. 8, 2017 Hearing, U.S. Senate Committee on
Commerce, Science & Transportation

TABLE OF CONTENTS

Financial Institution Plaintiffs ("FI Plaintiffs") (identified below), individually and on behalf of the Class defined below, and the Association Plaintiffs (identified below), individually acting on behalf of their members ("Association Plaintiffs") (collectively "Plaintiffs"), based on personal knowledge as to themselves and their own acts, on information and belief where indicated, and upon investigation of counsel as to all other matters, bring this putative class action against Equifax Inc. and Equifax Information Services LLC ("Equifax" or "Defendants"), and allege as follows:

INTRODUCTION

1. "*Powering the World with Knowledge.*" Equifax serves as a linchpin of the U.S. economy. By aggregating consumer data, Equifax enables financial institutions to extend credit and other financial services to U.S. consumers. Equifax heralds itself as a "trusted steward" that complies with the laws requiring Equifax to adequately safeguard consumer data. In reality, Equifax prioritized profits over privacy, exposing the information it acknowledged was responsible for powering the world.

2. FI Plaintiffs bring this class action to recover the financial losses they already have suffered as a result of the fraudulent banking activity that FI Plaintiffs have experienced and the certainly impending risk of future harm that is likely to

occur as a direct result of Equifax's egregious negligent mishandling of highly sensitive, personally identifiable information ("PII") and payment card data ("Payment Card Data").

3. Equifax's senior management ignored specific warnings that its systems were vulnerable to attack and refused to take the necessary steps to adequately protect consumer data. As a direct result of Equifax's weak cybersecurity measures, between at least May and July 2017, hackers stole the highly sensitive PII of approximately 147.9 million U.S. consumers – roughly 46% of the U.S. population and nearly 60% of all adults in the U.S. (the "Data Breach"). The Equifax Data Breach is arguably the most damaging data breach in this country's history, impacting at least one family member in ***every*** U.S. household. This PII includes but is not limited to:

a. names;

b. Social Security numbers;

c. birth dates;

d. addresses;

e. driver's license numbers;

f. images of taxpayer ID cards, passports or passport cards, and other government-issued identification documents;

g. photographs associated with these forms of government-issued identification; and

h. Payment Card Data, including, but not limited to, credit and debit card numbers, primary account numbers ("PANs"), card verification value numbers ("CVVs"), expiration dates, and zip codes.

4. This Data Breach shocks the conscience. Equifax fully understood its duties to protect the confidentiality, accuracy, and integrity of PII. Equifax fully understood that the threat of a data breach was a legitimate risk, and that if one occurred, the consequences would be severe and would directly impact FI Plaintiffs and the Class. Yet time and time again, Equifax refused to take the necessary steps to adequately protect consumer data. Indeed, in the months prior to the Data Breach, Equifax was subject to no fewer than five data breach incidents in which PII was compromised. It even received notification of the specific vulnerability that led to the Data Breach.

5. The Equifax Data Breach was a direct consequence of Equifax's deliberate decisions not to adopt recommended data security measures, decisions that left PII vulnerable. Equifax's data security deficiencies were so significant that the hackers' activities went undetected for at least two months. During that time,

the hackers had unfettered access to exfiltrate likely hundreds of millions of lines of consumer data. Had Equifax adopted reasonable data security measures, it could have prevented the Data Breach.

6. Equifax's former Chief Executive Officer ("CEO") Richard Smith admitted: "We at Equifax clearly understood that the collection of American consumer information and data carries with it enormous responsibility to protect that data. We did not live up to that responsibility[.] . . . Equifax was entrusted with Americans' private data and we let them down."[1]

7. Equifax knew that if it were to suffer a data breach, the repercussions would extend throughout the financial services industry. The compromised PII, like the compromised Payment Card Data, is precisely the data needed for thieves to commit fraud, by enabling them to illegitimately open accounts or hack into existing

[1] Oversight of the Equifax Data Breach: Answers for Consumers: Hearing before the U.S. House Committee on Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection (Oct. 3, 2017) (Prepared Testimony of Richard F. Smith), https://democrats-energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/Testimony-Smith-DCCP-Hrg-on-Oversight-of-the-Equifax-Data-Breach-Answers-for-Consumers-2017-10-03.pdf [hereinafter *Smith Testimony*].

accounts, apply for credit and loans, and withdraw or transfer funds with the stolen PII, which results in direct out-of-pocket costs to FI Plaintiffs and the Class.[2]

8. FI Plaintiffs and the Class have been injured, suffering financial losses directly attributable to the Data Breach. Specifically, because their customers' PII and/or Payment Card Data was compromised in the Data Breach, FI Plaintiffs and the Class have incurred direct out-of-pocket costs associated with: cancelling and reissuing compromised payment cards; reimbursing customers whose payment cards were compromised in the Data Breach for fraudulent transactions; reimbursing customers whose PII was stolen in the Data Breach for fraudulent transactions; lost revenues due to abandoned credit applications from customers who froze their credit reports in the wake of the Data Breach and were subsequently unable to unfreeze their credit reports in a timely fashion; increased staffing to respond to theft of customers' PII in the wake of the Data Breach; enhancing their customer verification procedures and retraining staff regarding these procedures; purchasing identity

[2] *The New Reality of Synthetic ID Fraud*, EQUIFAX INC., https://www.equifax.com/assets/IFS/syntheticID-fraud_wp.pdf (last accessed May 30, 2018); Daniel Jean, *The Impact of Synthetic Identity Fraud… By the Numbers*, INSIGHTS BLOG (April 19, 2018), https://insight.equifax.com/impact-synthetic-identity-fraud/; Cathleen Donahoo, *How Fraudsters Are Using Synthetic Identities*, INSIGHTS BLOG (March 28, 2018), https://insight.equifax.com/how-fraudsters-are-using-synthetic-identities/.

authentication, identity theft protection, or fraud detection and prevention software tools; and/or purchasing cyber security insurance. The out-of-pocket costs each FI Plaintiff specifically incurred are detailed below.

9. In light of the fraudulent banking activity that FI Plaintiffs and the Class already have experienced and out-of-pocket costs that FI Plaintiffs and the Class already have suffered, there exists a certainly impending risk of future harm, in the form of future fraudulent banking activity, as a direct result of the Equifax Data Breach. This risk of harm has required FI Plaintiffs and the Class to incur significant costs and expenses in order to reduce and mitigate this risk of harm. Finally, due to Equifax's long-term, gross inadequacy of Equifax's data security measures, which FI Plaintiffs allege have not been remedied, there exists a certainly impending risk of future harm to FI Plaintiffs and the Class that would result if Equifax experiences another data breach.

10. FI Plaintiffs, individually and on behalf of a nationwide class, seek to recover their damages as well as obtain non-monetary relief to require Equifax to enhance their data security measures and correct the glaring deficiencies that directly led to this Data Breach. FI Plaintiffs assert claims against Equifax for negligence (Count 1), negligence per se (Count 2), and negligent misrepresentation (Count 3). Additionally, FI Plaintiffs named in Counts 4-8, individually and on behalf of

statewide subclasses, seek monetary and non-monetary relief and assert claims for violation of various state unfair and deceptive business practices statutes. FI Plaintiffs, individually and on behalf of a nationwide class, along with the Association Plaintiffs, also request a declaratory judgment (Count 9). Finally, Plaintiffs seek to recover reasonable attorneys' fees and the expenses of litigation (Count 10).

PARTIES

FI Plaintiffs

11. Plaintiff ASI Federal Credit Union is a federally-chartered credit union with a principal place of business in Harahan, Louisiana, and is a citizen of Louisiana. Plaintiff ASI Federal Credit Union has customers whose PII was compromised in the Data Breach. As a result of the compromise of members' PII, Plaintiff ASI Federal Credit Union experienced an increase in fraudulent banking activity causing the institution to charge off the fraudulent transactions. As a result of the increased fraudulent banking activity it suffered and in direct response to the Data Breach, Plaintiff ASI Federal Credit Union incurred direct, out-of-pocket costs to purchase a fraud detection service from PULSE debit card network, costing approximately $500 per month. Plaintiff ASI Federal Credit Union also received at least one fraud alert from Visa notifying it that payment cards that it issued were

compromised due to the Data Breach. Therefore, Plaintiff ASI Federal Credit Union cancelled and reissued the payment cards that were identified by Visa as compromised in the Equifax Data Breach, and thereby, incurred direct out-of-pocket costs. Further, in response to customer requests in the immediate wake of the Equifax Data Breach, Plaintiff ASI Federal Credit Union cancelled and reissued 649 payment cards held by customers whose PII was compromised in the Data Breach.

12. Plaintiff Consumers Cooperative Credit Union is a state-chartered credit union with a principal place of business in Gurnee, Illinois, and is a citizen of Illinois. Plaintiff Consumers Cooperative Credit Union has customers whose PII was compromised in the Data Breach. In the aftermath of the Data Breach, Plaintiff Consumers Cooperative Credit Union experienced a marked increase in fraudulent banking activity using customers' PII that was compromised in the Data Breach. As a result of the fraudulent banking activity it suffered due to the Data Breach, Plaintiff Consumers Cooperative Credit Union incurred direct out-of-pocket costs to purchase identity authentication and identity theft protection services, specifically Transunion's service that provides knowledge based authentication through "out of wallet" questions, costing approximately $375,000 per year, and PSCU's Pindrop service, which identifies and prevents call center authentication fraud, costing approximately $20,000 per year. Also as a result of the fraudulent banking activity

it suffered due to the PII compromised by the Data Breach, Plaintiff Consumers Cooperative Credit Union implemented additional procedures to verify customers' identities, which resulted in direct out-of-pocket costs, including costs relating to adding two new staff members, costing approximately $100,000, and ten temporary customer services representatives to handle the work flow related to these additional measures. Plaintiff Consumers Cooperative Credit Union also received at least one fraud alert from Visa notifying it that payment cards that it issued were compromised due to the Data Breach. Therefore, Plaintiff Consumers Cooperative Credit Union incurred direct, out-of-pocket costs related to reimbursement of its customers for fraud associated with compromised payment cards and with cancelling and reissuing its payment cards that were identified by Visa as compromised in the Equifax Data Breach.

13. Plaintiff DL Evans Bank ("DL Evans") is a community bank with its principal place of business in Burley, Idaho and is a citizen of Idaho. Plaintiff DL Evans has customers whose PII was compromised in the Data Breach. Plaintiff DL Evans has incurred a significant increase in fraudulent banking activity, using customers' PII that was compromised in the Data Breach. As a result of the fraudulent banking activity it suffered due to the Data Breach, Plaintiff DL Evans has spent an extra approximately $88 per month in personnel time to deter fraud

attempts that occur on current accounts through a method known as "phishing." Plaintiff DL Evans also has customers whose PII was compromised in the Data Breach and who subsequently placed freezes on their credit reports as a result of the Data Breach. Due to this, Plaintiff DL Evans has incurred increased staffing costs and suffered lost revenues because customers who froze their credit reports in the wake of the Data Breach and were unable to unfreeze their credit reports in a timely fashion and the resultant delay in loans associated therewith. For example, one customer who froze his credit due to the Data Breach attempted to renew his line of credit with Plaintiff DL Evans, but did not know his PIN to unfreeze his credit. Plaintiff DL Evans spent time working with the customer to assist him in this endeavor, which ultimately required awaiting a new PIN by mail. The process took over two weeks, causing lost revenue of approximately $386.90 due to the delays and resulting in increased operating costs of $37.65 for Plaintiff DL Evans. Accordingly, Plaintiff DL Evans suffered direct out-of-pocket costs as a result of the PII compromised by the Data Breach.

14. Plaintiff Financial Health Federal Credit Union is a federally-chartered credit union with a principal place of business in Indianapolis, Indiana, and is a citizen of Indiana. Plaintiff Financial Health Federal Credit Union has customers whose PII was compromised in the Data Breach and who subsequently placed

freezes on their credit reports. As a result, Plaintiff Financial Health Federal Credit Union suffered lost revenues of approximately $13,000 due to abandoned credit applications from customers who froze their credit reports in the wake of the Data Breach and were unable to unfreeze their credit reports in a timely fashion. Specifically, in two instances, customers abandoned auto loan applications with Plaintiff Financial Health Federal Credit Union because the car each respectively wished to purchased had been sold off the car lot by the time that each was able to unfreeze their respective credit report. Also, as a result of customers freezing their credit reports in the aftermath of the Data Breach, it now takes Plaintiff Financial Health Federal Credit Union significantly more time to process auto loan applications. Prior to the Data Breach, auto loans were processed the same day. Now, as a result of the Data Breach and compromise of Plaintiff's customers' PII, auto loans take multiple days and increased staff time to process due to the added time it takes customers to unfreeze their credit reports. As a result of its customers' PII being compromised in the Data Breach, Plaintiff Financial Health Federal Credit Union has incurred direct out-of-pocket costs to enhance its customer verification procedures and retrain staff regarding these procedures and to purchase a cyber-insurance policy.

15. Plaintiff First Financial Credit Union is a state-chartered credit union with a principal place of business in Albuquerque, New Mexico, and is a citizen of New Mexico. Plaintiff First Financial Credit Union has customers whose PII was compromised in the Data Breach. In the aftermath of the Data Breach, Plaintiff First Financial Credit Union experienced fraudulent banking activity using customers' PII that was compromised in the Data Breach. As a result of the fraudulent banking activity it suffered due to the PII compromised by the Data Breach, Plaintiff First Financial Credit Union incurred direct out-of-pocket costs to reimburse customers whose PII was stolen in the Data Breach for fraudulent transactions involving checking accounts, costing approximately $2,500. Also as a result of the fraudulent banking activity it suffered due to the Data Breach, Plaintiff First Financial Credit Union incurred direct out-of-pocket costs to purchase, from Fidelity Information Services, LLC, an identity authentication and identity theft protection service that uses "out of wallet" questions to enhance the customer verification process, costing approximately $3,051.00. Relatedly, Plaintiff First Financial Credit Union also incurred direct out-of-pocket costs to retrain its staff regarding its enhanced customer and credit verification procedures.

16. Plaintiff The First State Bank is a state chartered community bank with its principal place of business in Barboursville, West Virginia and is a citizen of

West Virginia. Plaintiff The First State Bank has customers whose PII was compromised in the Data Breach. In the aftermath of the Data Breach, Plaintiff The First State Bank experienced fraudulent banking activity using customers' PII that was compromised in the Data Breach. As a direct result of the Data Breach, and consistent with guidance provided by experts and regulators to banks in the wake of the Data Breach, Plaintiff The First State Bank revised its authentication policies and procedures for customer accounts after the Data Breach and as a direct result of the Data Breach. Plaintiff The First State Bank moved away from using authentication questions that relied on the types of PII exposed in the Data Breach and now uses enhanced authentication methods to verify new and existing customers. The cost to The First State Bank for this change in policy and related training was approximately $4,500. As a direct result of the Data Breach, The First State Bank also began using a service called Data Verify, a data validation service, for all of its non-commercial lending, a practice the institution applied only to mortgages prior to the Data Breach. Plaintiff The First State Bank has suffered direct out-of-pocket costs resulting from the use of this service, which costs approximately $50 per loan application. Plaintiff The First State Bank also has customers whose PII was compromised in the Data Breach and who subsequently placed freezes on their credit reports as a result of the Data Breach. Plaintiff The First State Bank has a wholesale mortgage network of

about 60 banks, in which there has been an increase in credit freezes related to the Data Breach, resulting in a significant slowdown in the lending process. Due to these credit freezes and the resultant delay in the lending process, Plaintiff The First State Bank has incurred increased staffing costs and suffered lost revenues. Accordingly, The First State Bank suffered direct out-of-pocket losses as a result of the Data Breach.

17. Plaintiff Hudson River Community Credit Union is a state-chartered credit union with a principal place of business in Corinth, New York, and is a citizen of New York. Plaintiff Hudson River Community Credit Union has customers whose PII was compromised in the Data Breach. In the aftermath of the Data Breach, Plaintiff Hudson River Community Credit Union experienced fraudulent banking activity using customers' PII that was compromised in the Data Breach. As a result of the fraudulent banking activity it suffered due to the Data Breach, Plaintiff Hudson River Community Credit Union incurred direct out-of-pocket costs to reimburse customers whose PII was stolen in the Data Breach for fraudulent transactions, costing approximately $30,824. As a result of its customers' PII being compromised in the Data Breach, Plaintiff Hudson River Community Credit Union has also incurred costs associated with enhancing its customer verification procedures and retraining staff regarding these procedures. Plaintiff Hudson River

Community Credit Union also received at least one alert from Visa notifying it that payment cards that it issued were compromised due to the Data Breach. Therefore, Plaintiff Hudson River Community Credit Union cancelled and reissued its payment cards that were identified by Visa as compromised in the Data Breach, and thereby, incurred direct out-of-pocket costs.

18. Plaintiff Peach State Federal Credit Union is a federally-chartered credit union with a principal place of business in Lawrenceville, Georgia, and is a citizen of Georgia. Plaintiff Peach State Federal Credit Union has customers whose PII and Payment Card Data was compromised in the Data Breach. As a result of the fraudulent banking activity it suffered due to the PII compromised by the Data Breach, Plaintiff Peach State Federal Credit Union has incurred costs of approximately $2,500 per month to enhance its customer verification procedures and retrain staff regarding these procedures in light of increased deposit fraud they are incurring. Additionally, Plaintiff Peach State Federal Credit Union also has customers whose PII was compromised in the Data Breach and who subsequently placed freezes on their credit reports as a result of the Data Breach. Due to this, Plaintiff Peach State Federal Credit Union had to expend additional time and resources to review loan applications due to customers who froze their credit reports in the wake of the Data Breach. Specifically, the delays resulting from customers

who froze their credit reports in the wake of the Data Breach has caused Plaintiff Peach State Federal Credit Union to incur increased staffing costs and suffer lost revenues of approximately $4,062 per month. Plaintiff Peach State Federal Credit Union also received at least one alert from Visa notifying it that payment cards that it issued were compromised due to the Data Breach. Plaintiff Peach State Federal Credit Union cancelled and reissued its payment cards that were identified by Visa as compromised in the Data Breach, and thereby, incurred direct out-of-pocket costs.

19. Plaintiff Texas First Bank is a community bank with its principal place of business in Texas City, Texas and is a citizen of Texas. Plaintiff Texas First Bank is a customer of Equifax and receives services relating to consumer and credit information. Plaintiff Texas First Bank has customers whose PII was compromised in the Data Breach. In the aftermath of the Data Breach, Plaintiff Texas First Bank experienced fraudulent banking activity using customers' PII that was compromised in the Data Breach. As a direct result of the Data Breach, and consistent with guidance provided by experts and regulators to banks in the wake of the Data Breach, Plaintiff Texas First Bank incurred direct out-of-pocket costs to hire a new employee dedicated to cybersecurity and attempted fraud training in order to deter fraud attempts that occur on current accounts as a result of the Data Breach. The out-of-pocket cost to Plaintiff Texas First Bank for the role this employee performs as a

direct result of the Data Breach is approximately $20,000 per year. Plaintiff Texas First Bank also received notification from Visa that payment cards it issued were compromised due to the Data Breach. Plaintiff Texas First Bank incurred direct out-of-pocket costs related to the monitoring and reissuance of its payment cards that were identified by Visa as compromised in the Data Breach. Accordingly, Plaintiff Texas First Bank suffered direct out-of-pocket losses as a result of the Data Breach.

20. Plaintiff The Summit Federal Credit Union is a federally-chartered credit union with a principal place of business in Rochester, New York, and is a citizen of New York. Plaintiff The Summit Federal Credit Union has customers whose PII was compromised in the Data Breach. In the aftermath of the Data Breach, Plaintiff The Summit Federal Credit Union experienced fraudulent banking activity using customers' PII that was compromised in the Data Breach. As a result of the fraudulent banking activity it suffered due to the PII compromised by the Data Breach, Plaintiff The Summit Federal Credit Union incurred direct out-of-pocket costs to reimburse customers whose PII was stolen in the Data Breach for fraudulent transactions, costing approximately $10,000. Also as a result of the fraudulent banking activity it suffered due to the Data Breach, Plaintiff The Summit Federal Credit Union incurred direct out-of-pocket costs to enhance its customer verification procedures and retrain staff regarding these procedures and also to increase staffing

costing Plaintiff approximately $55,000 to handle customer verifications, which now require substantial additional information from customers. Plaintiff The Summit Federal Credit Union also received at least one alert from Visa notifying it that payment cards that it issued were compromised due to the Data Breach. Therefore, Plaintiff The Summit Federal Credit Union cancelled and reissued its payment cards that were identified by Visa as compromised in the Data Breach, and thereby, incurred direct out-of-pocket costs.

21. Plaintiff TruEnergy Federal Credit Union f/k/a Washington Gas Light Federal Credit Union is a federally-chartered credit union with a principal place of business in Springfield, Virginia, and is a citizen of Virginia. Plaintiff TruEnergy Federal Credit Union has customers whose PII and payment card data were compromised in the Data Breach. In the aftermath of the Data Breach, Plaintiff TruEnergy Federal Credit Union experienced fraudulent banking activity using customers' PII and payment card data that was compromised in the Data Breach. As a result of the fraudulent banking activity it suffered due to the Data Breach, Plaintiff TruEnergy Federal Credit Union incurred direct, out-of-pocket costs to purchase from Fiserv its Risk Office Advisor Bundle to detect and prevent payment card fraud, costing approximately $10,500 to date. Relatedly, Plaintiff TruEnergy Federal Credit Union also incurred direct, out-of-pocket costs to retrain its staff

regarding its enhanced customer and credit verification procedures. Plaintiff TruEnergy Federal Credit Union also has customers whose PII and payment card data was compromised in the Data Breach and who subsequently placed freezes on their credit reports as a result of the Data Breach. Due to this, Plaintiff TruEnergy Federal Credit Union has had to expend additional time and resources and likely suffered lost revenues due to customers who froze their credit reports in the wake of the Data Breach and were unable to unfreeze their credit reports in a timely fashion and the resultant delay in loans associated therewith. In addition, in response to the Data Breach, Plaintiff TruEnergy Federal Credit Union has had to expend additional time and resources in connection with notifying customers that their payment cards were compromised, verifying its customers' identity prior to approving transactions, and has implemented a 10-day hold on any ACH transactions for credit card payments in the amount of $500 or more in response to the Data Breach after having attempted ACH fraud of approximately $17,700 on its members that were victims of the Data Breach or had payment cards compromised in the Data Breach. Plaintiff TruEnergy Federal Credit Union has also received two alerts from Visa notifying it that payment cards that it issued were compromised due to the Data Breach. Therefore, Plaintiff has had to expend additional time and resources and incurred

direct, out-of-pocket costs related to the reissuance of its payment cards that were compromised in the Data Breach.

Association Plaintiffs

22. The Association Plaintiffs are associations or leagues whose financial institution members have suffered harm resulting from the compromise of their members' consumer data, including FI Plaintiffs' customers' PII and/or Payment Card Data that was compromised in the Data Breach. The Association Plaintiffs' members also are subject to a certainly impending risk of future harm, in the form of future fraudulent banking activity, as a direct result of the compromised PII and PCD associated with the Equifax Data Breach. As a direct consequence of the Equifax Data Breach, the Association Plaintiffs' members have suffered direct out-of-pocket costs, as described above in Paragraphs 11 - 21, and are subject to a greater risk of fraudulent banking activity, which will continue into the foreseeable future, that has required the Association Plaintiffs' members to incur significant costs and expenses.

23. The Association Plaintiffs are non-class plaintiffs. While the Association Plaintiffs have been injured by the Equifax Data Breach, they do not seek money damages. Rather, the Association Plaintiffs bring this action for equitable relief on behalf of their members. The Association Plaintiffs are as follows:

24. Plaintiff Credit Union National Association ("CUNA") is a Wisconsin trade association whose members include credit unions that operate in all fifty states. CUNA's members have standing to sue in their own right and include the following FI Plaintiffs: ASI Federal Credit Union, Consumers Cooperative Credit Union, Financial Health Federal Credit Union, First Financial Credit Union, Hudson River Community Credit Union, Peach State Federal Credit Union, The Summit Federal Credit Union, and TruEnergy Federal Credit Union. As described above, in Paragraphs 11, 12, 14, 15, 17, 18, 20, & 21, these FI Plaintiffs have incurred direct out-of-pocket costs associated with: cancelling and reissuing compromised payment cards; reimbursing customers whose payment cards were compromised in the Data Breach for fraudulent transactions; reimbursing customers whose PII was stolen in the Data Breach for fraudulent transactions; lost revenues due to abandoned credit applications from customers who froze their credit reports in the wake of the Data Breach and were subsequently unable to unfreeze their credit reports in a timely fashion; increased staffing to respond to theft of customers' PII in the wake of the Data Breach; enhancing their customer verification procedures and retraining staff regarding these procedures; purchasing identity authentication, identity theft protection, or fraud detection and prevention software tools; and/or purchasing cyber security insurance. CUNA brings this action as an association on behalf of its

members. CUNA has standing to assert its claims on behalf of its members because: (a) as alleged above for ASI Federal Credit Union, Consumers Cooperative Credit Union, Financial Health Federal Credit Union, First Financial Credit Union, Hudson River Community Credit Union, Peach State Federal Credit Union, The Summit Federal Credit Union, and TruEnergy Federal Credit Union, its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to its purpose of, among other things, supporting initiatives that promote the financial stability of its members; and (c) the participation of its members is not needed in order to obtain the injunctive relief requested. CUNA also has standing to assert its claims because it was forced to divert and expend its own resources to assist members that have been harmed and continue to be harmed by the Equifax Data Breach. As a result of the Data Breach, CUNA diverted resources that normally would have been spent on outreach efforts relating to advocacy, regulatory and legislative initiatives, tax issues, technology, education and training, to communicate with its members about the increased risk of fraudulent banking activity that was likely to occur (and now has occurred), how to evaluate their identity authentication safeguards, how to monitor for and identify application fraud and account takeovers through call centers and online functionalities on the member websites, whether to continue reporting data to Equifax, and what to communicate

to customers about identity theft and freezing/unfreezing credit reports and how to train staff to engage in these communications. Additionally, the Data Breach has caused CUNA to divert monies to create a data breach toolkit for its members, and to sponsor a webinar for its members to educate them regarding the Equifax Data Breach.

25. Plaintiff Independent Community Bankers of America ("ICBA") is headquartered in Washington, DC, and is the primary trade association for community banks of all sizes and charter types. ICBA is the voice for nearly 5,700 community banks nationwide. ICBA's members have standing to sue in their own right, including Plaintiffs DL Evans Bank, First State Bank, and Texas First Bank. As described above, in Paragraphs 13, 16, & 19, these FI Plaintiffs have incurred direct out-of-pocket costs associated with: a significant increase in attempted fraud, using the PII compromised in the Data Breach resulting in additional costs in personnel time to deter these attempts, increased staffing costs and lost revenues resulting from assisting customers who subsequently placed freezes on their credit reports as a result of the Data Breach, and costs associated with monitoring and reissuance of payment cards that were compromised in the Data Breach. ICBA brings this action as an association on behalf of its members and the community banks whose interests it represents. ICBA has standing to assert its claims on behalf

of its members because: (a) as alleged above for Plaintiffs DL Evans Bank, First State Bank, and Texas First Bank, its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to its purpose of, among other things, supporting initiatives that promote the financial stability of its members; and (c) the participation of its members is not needed in order to obtain the injunctive relief requested. ICBA also has standing to assert its claims because it was forced to divert and expend its own resources to assist members that have been harmed and continue to be harmed by the Equifax Data Breach. As a result of the Data Breach, ICBA diverted resources that normally would have been spent on advocacy, education, compliance and enhancing services offered to its community bank members, to communicate with its members about the increased risk of fraudulent banking activity that was likely to occur (and now has occurred), how to educate its members to enhance data cyber security training, and how to assist members and their customers to protect their data and safeguard personal information against theft. For example, ICBA hosted multiple conference calls with its members to discuss the Data Breach, its effect on ICBA members, and its members' response to the Data Breach. It communicated with Equifax regarding the Data Breach, its effect on ICBA members and their customers, Equifax's response to the Data Breach, and with a request for information on any actions being

taken by Equifax in response to the Data Breach. ICBA also devoted resources to legislative and regulatory initiatives proposed specifically in response to the Data Breach.

26. Plaintiff Illinois Credit Union League ("Illinois CUL") is an Illinois trade association whose members are credit unions that operate in Illinois. Illinois CUL's members have standing to sue in their own right, including Plaintiff Consumers Cooperative Credit Union. As described above, in Paragraph 12, Plaintiff Consumers Cooperative Credit Union has incurred direct out-of-pocket costs to purchase identity authentication and identity theft protection services, implemented additional procedures to verify customers' identities, which resulted in direct out-of-pocket costs, and incurred direct out-of-pocket costs related to the reissuance of its payment cards and reimbursing customers whose payment card data was compromised in Data Breach for fraudulent transactions. Illinois CUL brings this action as an association on behalf of its members. Illinois CUL has standing to assert its claims on behalf of its members because: (a) as alleged above with respect to Plaintiff Consumers Cooperative Credit Union, its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to its purpose of, among other things, supporting initiatives that promote the financial stability of its members; and (c) the participation of its members is not

needed in order to obtain the injunctive relief requested. Illinois CUL also has standing to assert its claims because it was forced to divert and expend its own resources to assist members that have been harmed and continue to be harmed by the Equifax Data Breach. As a result of the Data Breach, Illinois CUL diverted resources that normally would have been spent on providing advocacy, information, legislative support, education and compliance resources to its members, to communicate with its members about the Data Breach and the increased risk of fraudulent banking activity that was likely to occur (and now has occurred), how to enhance the protection of personal information and monitor for identity theft and credit fraud, what to communicate to customers about identity theft and freezing/unfreezing credit reports, and how to educate and to train staff to respond to member communications.

27. Plaintiff Indiana Credit Union League ("Indiana CUL") is an Indiana trade association whose members are credit unions that operate in Indiana. Indiana CUL's members have standing to sue in their own right, including Plaintiff Financial Health Federal Credit Union. As described above, in Paragraph 14, this FI Plaintiff has incurred direct out-of-pocket costs associated with: abandoned credit applications from customers who froze their credit reports in the wake of the Data Breach, direct out-of-pocket costs to enhance its customer verification procedures

and retrain staff regarding these procedures, and to purchase a cyber-insurance policy. Indiana CUL brings this action as an association on behalf of its members. Indiana CUL has standing to assert its claims on behalf of its members because: (a) as alleged above with respect to Plaintiff Financial Health Federal Credit Union, its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to its purpose of, among other things, supporting initiatives that promote the financial stability of its members; and (c) the participation of its members is not needed in order to obtain the injunctive relief requested. Indiana CUL also has standing to assert its claims because it was forced to divert and expend its own resources to assist members that have been harmed and continue to be harmed by the Equifax Data Breach. As a result of the Data Breach, Indiana CUL diverted resources that normally would have been spent on advocacy, compliance, education and legislative efforts for its members, to collect information from members relating to the impact of the Data Breach, communicate with its members about the increased risk of fraudulent banking activity that was likely to occur (and now has occurred), and how to assist members and their customers to safeguard their personal information and Payment Card Data.

28. Plaintiff New York Credit Union Association ("NYCUA") is a New York trade association whose members are credit unions that operate in New York.

NYCUA's members have standing to sue in their own right, including Plaintiffs Hudson River Community Credit Union and The Summit Federal Credit Union. As described above, in Paragraphs 17 and 20, these FI Plaintiffs have incurred direct out-of-pocket costs associated with: incurred direct out-of-pocket costs to reimburse customers whose PII was stolen in the Data Breach for fraudulent transactions, enhancing its customer verification procedures and retraining staff regarding these procedures, and direct out-of-pocket costs related to the reissuance of its payment cards that were identified as compromised in the Data Breach. NYCUA brings this action as an association on behalf of its members. NYCUA has standing to assert its claims on behalf of its members because: (a) as alleged above with respect to Plaintiffs Hudson River Community Credit Union and The Summit Federal Credit Union, its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to its purpose of, among other things, supporting initiatives that promote the financial stability of its members; and (c) the participation of its members is not needed in order to obtain the injunctive relief requested. NYCUA also has standing to assert its claims because it was forced to divert and expend its own resources to assist members that have been harmed and continue to be harmed by the Equifax Data Breach. As a result of the Data Breach, NYCUA diverted resources that normally would have been spent on advocacy,

education, and legislative efforts, to communicate with its members about the Data Breach and the increased risk of fraudulent banking activity that was likely to occur (and now has occurred), and educating and communicating with its members regarding the increased risks associated with identity theft and fraudulent transactions as a result of the Data Breach.

29. Plaintiff Virginia Credit Union League ("Virginia CUL") is a Virginia trade association whose members are credit unions that operate in Virginia. Plaintiff Virginia CUL's members have standing to sue in their own right, including Plaintiff TruEnergy Federal Credit Union. As described above, in Paragraph 21, this FI Plaintiff has incurred direct out-of-pocket costs associated with: reimbursing customers whose PII was stolen in the Data Breach for fraudulent transactions, identity authentication and identity theft protection service, retraining staff regarding its enhanced customer and credit verification procedures, and direct out-of-pocket costs related to the reissuance of its payment cards that were identified as compromised in the Data Breach. Virginia CUL brings this action as an association on behalf of its members. Virginia CUL has standing to assert its claims on behalf of its members because: (a) as alleged above with respect to Plaintiff TruEnergy Federal Credit Union, its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to its purpose of, among

other things, supporting initiatives that promote the financial stability of its members; and (c) the participation of its members is not needed in order to obtain the injunctive relief requested. Virginia CUL also has standing to assert its claims because it was forced to divert and expend its own resources to assist members that have been harmed and continue to be harmed by the Equifax Data Breach. As a result of the Data Breach, Virginia CUL diverted resources that normally would have been spent on advocacy, consulting, compliance, and education services offered to its members, to communicate with its members about the increased risk of fraudulent banking activity that was likely to occur (and now has occurred), and how to educate its members regarding credit freezes and how to assist members and their customers to protect their PII an PCD.

30. The Association Plaintiffs are duly authorized to bring this action against Equifax. Many of the Association Plaintiffs' members do not have the time or resources to pursue this litigation and fear retribution if they were to become named plaintiffs. Equifax has caused the Association Plaintiffs to divert and expend their own resources to assist members that have been harmed and continue to be harmed by the Equifax data breach, and they have been otherwise directly and adversely impacted.

Defendants

31. Defendant Equifax Inc. ("Equifax Inc.") is a publicly-traded corporation with its principal place of business at 1550 Peachtree Street, NW, Atlanta, Georgia. Equifax Inc. represents that it is a leading global provider of information solutions and human resources business process outsourcing services for businesses, governments, and consumers. Equifax further represents that its customers include financial institutions, corporations, governments, and individuals and that it offers products and services based on its comprehensive databases of consumer and business information derived from numerous sources including credit, financial assets, telecommunications and utility payments, employment, income, demographic, and marketing data.

32. Defendant Equifax Information Services LLC ("EIS") is a wholly-owned subsidiary of Equifax Inc. with its principal place of business at 1550 Peachtree Street, NW, Atlanta, Georgia. EIS collects and reports consumer information to financial institutions, including FI Plaintiffs and the Classes.

33. Defendants operate together as a consumer reporting agency ("CRA") to prepare and furnish consumer reports for credit and other purposes.

34. Equifax Inc. and its subsidiaries have eliminated nearly all corporate lines between their formal business entities in the collection, maintenance, sharing,

and furnishing of consumer reporting information. Equifax Inc. entities such as EIS regularly and freely share confidential consumer information with sibling entities so all entities, and ultimately Equifax Inc., can market and profit from the sale of information solutions and consumer identity theft protection products.

35. Throughout the events at issue here, Defendants have operated as one entity and CRA. As it pertains to consumer reporting, Equifax Inc. has used EIS as a dependent and integrated division rather than as a separate legal entity. The business operations are fully coordinated and shared. Resources are cross-applied without recognizing full and complete cost and profit centers. Management decisions at EIS are made by and through management of Equifax Inc. The management of Equifax Inc. was and is directly involved in the events at issue in this litigation, including Equifax's cybersecurity, the Data Breach itself, and Defendants' response to the Data Breach.

36. To remain separate and distinct for the purposes of liability in this action, Defendants must operate as separate and distinct legal and operational entities. Here, for the matters and functions alleged and relevant herein, EIS was merely an alter ego of Equifax Inc. For purposes of how consumer data was handled, warehoused, used, and sold, the corporate distinctions were disregarded in practice. EIS was a mere instrumentality for the transaction of the corporate consumer credit

business. Defendants shared full unity of interest and ownership such that the separate personalities of the corporation and subsidiary no longer existed.

37. Further, recognition of the technical corporate formalities in this case would cause irremediable injustice and permit Equifax Inc. – the entity whose management caused and permitted the events alleged herein – to defeat justice and to evade responsibility. *See Derbyshire v. United Builders Supplies, Inc.*, 194 Ga. App. 840, 844 (1990).

38. Accordingly, for all purposes hereafter, when Plaintiffs allege "Equifax" as the actor or responsible party, they are alleging the participation and responsibility of Equifax Inc. and EIS collectively.

JURISDICTION AND VENUE

39. This Court has original jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d). The aggregated claims of the individual class members exceed the sum or value of $5,000,000 exclusive of interest and costs; there are more than 100 putative class members defined below; and minimal diversity exists because the majority of putative class members are citizens of a different state than Defendants.

40. This Court has personal jurisdiction over Defendants because they maintain their principal headquarters in Georgia, their executives are located in

Georgia, they are registered to conduct business in Georgia, regularly conduct business in Georgia, and have sufficient minimum contacts in Georgia. Defendants intentionally avail themselves of this jurisdiction by conducting their corporate operations here and promoting, selling, and marketing Equifax products and services to resident Georgia financial institutions, consumers, and other entities. Moreover, the decisions which led to the Data Breach were made by executives and employees located in Georgia.

41. Venue is proper in this District under 28 U.S.C. §1391(a) because Defendants' principal places of business are in Georgia, and a substantial part of the events, acts, and omissions giving rise to the claims of Plaintiffs occurred in this District.

FACTUAL ALLEGATIONS

As One of the "Big Three" CRAs, Equifax Is at the Center of the Credit-Based U.S. Economy

42. Equifax is one of the "big three" CRAs, along with Experian and TransUnion. CRAs, including Equifax, accumulate data relating to consumers from various sources; compile that data in a usable format known as a credit report; and sell access to those reports to lenders interested in making credit decisions as well as financial companies, employers, and other entities that use those reports to make decisions about individuals in a range of areas. Because the extension of credit relies

on access to consumers' credit files, the CRAs have been referred to as the "linchpins" of the U.S. financial system.[3]

43. In a consumer credit system, financial institutions provide the means for consumers to borrow money or incur debt, and to defer repayment of that money over time. The provision of credit by financial institutions enables consumers to buy goods or assets without having to pay for them in cash at the time of purchase.[4] Nearly all Americans rely on credit to make everyday purchases using credit cards, obtain student loans and further education, gain approval for items like cellular phones and Internet access, and to make major life purchases such as automobiles and homes.

---

[3] AnnaMaria Andriotis, Michael Rapoport, & Robert McMillan, '*We've Been Breached': Inside the Equifax Hack*, THE WALL STREET JOURNAL (Sept. 18, 2017), https://www.wsj.com/articles/weve-been-breached-inside-the-equifax-hack-1505693318.

[4] M. Greg Braswell and Elizabeth Chernow, *Consumer Credit Law & Practice in the U.S.*, THE U.S. FEDERAL TRADE COMMISSION at 1, https://www.ftc.gov/sites/default/files/attachments/training-materials/law_practice.pdf (last accessed May 29, 2018) [hereinafter FTC, *Consumer Credit Law & Practice in the U.S.*].

44. "The U.S. credit reporting system encompasses a vast flow and store of information."[5] Indeed, "[c]redit report accuracy relies on an ongoing ecosystem involving the interaction of [CRAs], furnishers of information, public record repositories, users of credit reports, and consumers."[6]

45. Today, creditors such as credit unions and banks, like FI Plaintiffs and the Class, loan money to consumers, track the consumers' payment history on the loan, and then provide that information to one or more CRAs. The CRAs track the payment history creditors submit relating to an individual consumer and compile that information into a consumer's credit reporting "file."[7]

46. A consumer's credit file contains identifying information such as the consumer's name, date of birth, address, and Social Security number, as well as payment information on past credit accounts, including the name of the lender, the original amount of the loan, the type of the loan, and how much money the consumer still owes on the loan. A credit file also contains information in the public record

---

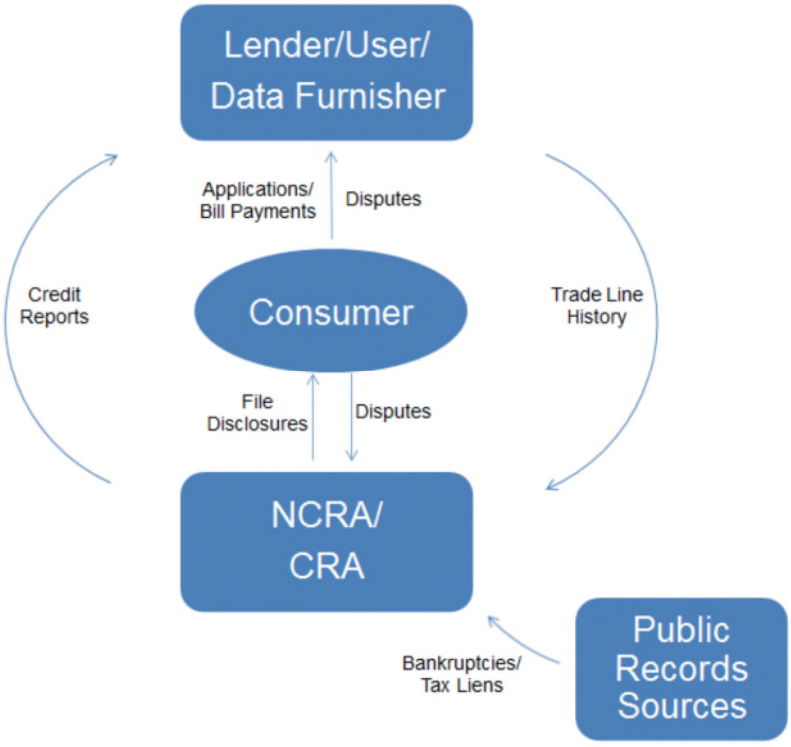
5 *Key Dimensions and Processes in the U.S. Credit Reporting System*, CONSUMER FINANCIAL PROTECTION BUREAU, at 3 (December 2012), https://files.consumerfinance.gov/f/201212_cfpb_credit-reporting-white-paper.pdf.

6 *Id.* at 6.

7 FTC, *Consumer Credit Law & Practice in the U.S.*, *supra* n.4 at 1.

that might affect the consumer's ability to pay back a loan, such as recent bankruptcy filings, pending lawsuits, or tax liabilities.[8]

47. The following depicts the flow of data among the participants in the consumer credit system: [9]



48. Financial institutions such as FI Plaintiffs and the Class make up the most significant segment of furnishers of data to the CRAs. According to a study

---

8 *Id*. at 1.

9 *Key Dimensions and Processes in the U.S. Credit Reporting System*, CONSUMER FINANCIAL PROTECTION BUREAU, at 13 (Dec. 2012), https://files.consumerfinance.gov/f/201212_cfpb_credit-reporting-white-paper.pdf.

by the Consumer Finance Protection Bureau ("CFPB"), approximately 40% of trade lines in the major CRAs' files relate to bank payment cards; 18% are from banks that issue retail cards; and the remainder are from collection agencies, debt buyers, the education industry, sales finance lenders, mortgage lenders, auto lenders, or other various creditors.[10]

49. Although the three nationwide CRAs collect information independently and do not have identical data, there is substantial overlap in their databases as a result of the standardization in reporting formats and the tendency of most major furnishers to report their consumer data to multiple CRAs.[11] Even if a particular furnisher or financial institution reports its customers' data to just one CRA, the other CRAs nevertheless can and often do possess much of the same PII for those same customers through consumer data received from other furnishers.[12]

50. FI Plaintiffs and the Class rely on the very PII elements that were exposed in the Equifax Data Breach, not only to determine a consumer's

---

10 *Id.* at 14.

11 *Report to Congress on the Fair Credit Reporting Act Dispute Process*, FEDERAL TRADE COMMISSION AND FEDERAL RESERVE BOARD, at 5 (Aug. 2006), https://www.federalreserve.gov/boarddocs/rptcongress/fcradispute/fcradispute200608.pdf.

12 This overlap in coverage is especially likely between Equifax and Experian, the largest two CRAs, because each possesses credit information on at least 800 million individuals.

creditworthiness, but also to verify the identity of their customers for all the financial services they offer. Indeed, when consumer PII is compromised resulting in fraudulent transactions, financial institutions like FI Plaintiffs and the Class are the ones who incur the losses as they reimburse their customers for such fraud, and incur additional out-of-pocket costs associated with protecting and safeguarding their customers' financial assets.

51. Consequently, the size and scope of Equifax's Data Breach has provided criminals access to all the data necessary to commit fraud, enabling them to illegitimately open or hack into existing accounts, apply for credit and loans, complete fraudulent transactions and transfer funds with customers' stolen PII, which results in direct out-of-pocket costs to FI Plaintiffs and the Class.

Equifax Compiles Massive Amounts of Consumer Data

52. Founded in 1899, Equifax is the oldest and second-largest CRA with $3.1 billion in revenue in 2016.[13] Over 25% of its revenue is generated from the services Equifax offers to its customers in the financial services industry, like FI

[13] Equifax Inc., Annual Report (Form 10-K) (Feb. 22, 2017) at 27.

Plaintiffs and the Class.[14] Equifax represents that it obtains and manages consumer data on over 820 million individuals and over 91 million businesses.[15]

53. Equifax's marketing motto is "Powering the World with Knowledge" and it claims to be "a leading global provider of information solutions . . . for businesses, governments and consumers."[16] To that end, Equifax states that it uses "advanced statistical techniques and proprietary software tools to analyze all available data, creating customized insights, decision-making solutions and processing services for our clients."[17]

54. According to Equifax, its "products and services are based on comprehensive databases of consumer and business information derived from numerous sources, including credit, financial assets, telecommunications and utility payments, employment, income, demographic and marketing data."[18] Credit card companies, banks, credit unions, retailers, auto and mortgage lenders all report the

14 *Id.* at 4.

15 *Id.* at 2.

16 *Id.*

17 *Id.*

18 *Id.*

details of consumer credit activity to Equifax.[19] In a speech at the University of Georgia, former Equifax CEO Richard Smith explained that Equifax gets its data for free because consumers hand it over to the banks when they apply for credit and that Equifax then crunches the data with the help of computer scientists and artificial intelligence and sells it back to the banks generating a gross margin of about 90 percent.[20]

55. Equifax takes the confidential, personal information that it collects and sells four primary data products: credit services, decision analytics, marketing services, and consumer assistance services.[21] In essence, Equifax's primary business asset is consumer data, which is in part comprised of PII data elements that Equifax algorithmically analyzes and sells to its customers.

---

19 *How Do Credit Reporting Agencies Get Their Information?* EQUIFAX INC., (July 2, 2014), https://blog.equifax.com/credit/how-do-credit-reporting-agencies-get-their-information/.

20 Michael Riley, Jordan Robertson, and Anita Sharpe, *The Equifax Hack Has the Hallmarks of State-Sponsored Pros*, BLOOMBERG (Sept. 29, 2017 9:09 AM), https://www.bloomberg.com/news/features/2017-09-29/the-equifax-hack-has-all-the-hallmarks-of-state-sponsored-pros.

21 Equifax Inc., Annual Report (Form 10-K) (Feb. 22, 2017) at 3.

Equifax Knows that Its Consumer Data Must Be Accurate and Adequately Safeguarded

56. Equifax acknowledges that it is "subject to numerous laws and regulations governing the collection, protection and use of consumer credit and other information, and imposing sanctions for the misuse of such information or unauthorized access to data," including the Fair Credit Reporting Act ("FCRA"), 18 U.S.C. §§1681, *et seq.*, the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§41, *et seq.*, Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. §§6801, *et seq.*, and state unfair and deceptive trade practices acts.[22]

57. Because of the widespread use of credit reports, the accuracy of such reports, and integrity of the information contained therein is an ongoing policy concern, as reflected in the FCRA, 18 U.S.C. §§1681, *et seq*., which governs the accuracy, fairness and privacy of information in the files of the CRAs. Equifax is subject to the FCRA as a CRA as defined in 15 U.S.C. §§1681a(f) and (p).

58. In the FCRA, Congress emphasized the need to maintain the integrity of the credit reporting system and recognized the dependence of the "banking system" as a whole on the reliability of credit reporting information:

---

[22] *Id*. at 10.

> **(a) Accuracy and fairness of credit reporting**.
>
> The Congress makes the following findings:
>
> (1) ***The banking system is dependent upon fair and accurate credit reporting. Inaccurate credit reports directly impair the efficiency of the banking system,*** and unfair credit reporting methods undermine the public confidence which is essential to the continued functioning of the banking system. [Emphasis added].
>
> (2) An elaborate mechanism has been developed for investigating and evaluating the credit worthiness, credit standing, credit capacity, character, and general reputation of consumers.
>
> (3) Consumer reporting agencies have assumed a vital role in assembling and evaluating consumer credit and other information on consumers.
>
> (4) There is a need to insure that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy.

15 U.S.C. §1681.

59. The FCRA also recognizes a duty to maintain reasonable procedures in order to protect the confidentiality, accuracy, and proper use of credit information.

> (b) Reasonable procedures
>
> It is the purpose of this subchapter to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of this subchapter.

15 U.S.C. §1681.

60. In a 2007 report on credit scores used in lending decisions, the Federal Reserve Board also commented on the importance of accurate credit reports, stating: "for the full benefits of the credit-reporting system to be realized, credit records must be reasonable, complete, and accurate."[23]

61. The accuracy of credit report information cannot be guaranteed without safeguards to maintain the confidentiality of consumer data. To this end, the GLBA regulates, among other things, the use of non-public personal information of consumers that is held by CRAs and financial institutions. The GLBA's provisions and implementing regulations include 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.

62. The Federal Trade Commission ("FTC") issued the Standards for Safeguarding Customer Information Rule ("Safeguards Rule"), 16 C.F.R. Part 314, to implement Section 501(b) of the GLBA, 15 U.S.C. §6801(b).

---

[23] *Report to Congress on Credit Scoring and its Effects on the Availability and Affordability of Credit*, FEDERAL RESERVE BOARD (Aug. 2007) (Board Credit Scoring Report), http://www.federalreserve.gov/boarddocs/rptcongress/creditscore/creditscore.pdf.

63. Equifax is subject to the requirements of the Safeguards Rule as a "financial institution," as that term is defined by Section 509(3)(A) of the GLBA, 15 U.S.C. §6809 (3)(A).

64. Section 501(b) of the GLBA, 15 U.S.C. §6801(b), requires Equifax to follow specific standards regarding the protection of customer information. Specifically, §6801(b) states:

> It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.
>
> (b) Financial institutions safeguards
>
> > In furtherance of the policy in subsection (a) of this section, each agency or authority described in section 6805(a) of this title shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards –
> >
> > 1) to insure the security and confidentiality of customer records and information;
> > 2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
> > 3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

65. The Safeguards Rule requires Equifax to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable

administrative, technical, and physical safeguards that include: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§314.3, 314.4.

66. As Equifax well knows, FI Plaintiffs and the Class also are governed by the accuracy and safeguards requirements of these laws. FI Plaintiffs and the Class are participants in the same regulatory regime described above as Equifax. Indeed, information provided by financial institutions to CRAs must be protected at every level. *See, e.g.*, Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. Part 225 App. F, 12 C.F.R Part 570 App. B, 12 C.F.R. Part 748

App. A, 12 C.F.R. Part 364 App. B, 12 C.F.R. Part 208 App. D-2, 12 C.F.R. Part 30 App. B.

67. Section 5 of the FTC Act, 15 U.S.C. §45, prohibits "unfair . . . practices in or affecting commerce." The FTC interprets Section 5 the FTC Act to require reasonable data security measures. Many states also have enacted similar statutes that require reasonable data security measures.

68. The foregoing statutes placed a duty on Equifax to act reasonably in managing consumer data and to use reasonable data security measures. In light of the foregoing regulatory regime and the following public statements, as well as Equifax's unique position in the credit reporting and financial services ecosystem, FI Plaintiffs and the Class reasonably relied on Equifax to safeguard consumer data so that such data remained accurate within the credit reporting and financial services ecosystem. Furthermore, as discussed below, Equifax fully intended FI Plaintiffs and the Class to so rely. Also, in light of the foregoing regulatory scheme, Equifax knew that FI Plaintiffs, as payment card issuers, lenders, and deposit account holders, would bear the ultimate responsibility for identity theft and fraudulent lending and other fraudulent consumer transactions.

Equifax Represents that Its Consumer Data Is Accurate and Is Adequately Safeguarded

69. Equifax actively recruits financial institutions, like FI Plaintiffs and the Class, to furnish their consumer data to Equifax, urging: "Reporting your data to Equifax supports the development of comprehensive consumer credit profiles, which benefits both consumers and the greater business community."[24] Equifax also emphasizes: "Furnishers who report data to Equifax play a vital role in helping identify credit risk and reduce financial losses throughout the entire credit granting community."[25]

70. Equifax says "Reporting Data is a Win-Win Situation," and specifically encourages financial institutions to furnish their consumer data to Equifax because it is "Safe, Simple, Secure."[26] One of the key benefits of furnishing data, according to Equifax, is that the customer can: "Gain more peace of mind by working with a

---

[24] *Prospective Data Furnishers Frequently Asked Questions*, EQUIFAX INC., https://assets.equifax.com/assets/usis/data_furnisher_faq.pdf (last accessed May 30, 2018).

[25] *Guidebook for Prospective Data Furnishers*, EQUIFAX INC., https://assets.equifax.com/assets/usis/data_furnisher_guidebook.pdf (last accessed May 30, 2018).

[26] *Consumer Data Reporting*, EQUIFAX INC., https://assets.equifax.com/assets/usis/dataFurnishersConsumerCreditData_ps.pdf (last accessed May 30, 2018).

trusted data provider ***with industry-leading data security and protection protocols***."[27] To this end, Equifax explains:

> Equifax is a trusted steward of credit information for thousands of financial institutions and businesses, and millions of consumers. ***We take this responsibility seriously, and follow a strict commitment to data excellence that helps lenders get the quality information they need to make better business decisions***.
>
> What's more, in today's environment of increasingly complex data privacy and security regulations, we provide businesses with more peace of mind and confidence when it comes to data reporting, and expert security compliance teams who are dedicated to data protection.[28] [Emphasis added].

71. Equifax readily acknowledges the importance of data furnished by financial institutions such as FI Plaintiffs and the Class, stating that the loss of such data is a risk factor to its business: "We rely extensively upon data from external sources to maintain our proprietary and non-proprietary databases, including data received from customers, strategic partners and various government and public record sources. This data includes the widespread and voluntary contribution of credit data from most lenders in the U.S."[29]

---

27 *Id.*

28 *Id.*

29 Equifax Inc., Annual Report (Form 10-K) (Feb. 22, 2017) at 15.

72. In its 2016 Form 10-K, Equifax touted itself as a "trusted steward and advocate for our customers and consumers" and stated that it was "continuously improving the customer and consumer experience in our consumer and commercial offerings, anticipating and executing on regulatory initiatives, while simultaneously delivering security for our services."[30] It also claimed: "Data is at the core of our value proposition."[31]

73. As to its regulatory obligations, Equifax acknowledged that it is "subject to numerous laws and regulations governing the collection, protection and use of consumer credit and other information, and imposing sanctions for the misuse of such information or unauthorized access to data," including the FCRA, FTC Act, GLBA, and state unfair and deceptive trade practices actions.[32]

74. Specifically, Equifax acknowledged that the "security measures we employ to safeguard the personal data of consumers could also be subject to the FTC Act."[33] It also admitted that it must comply with the FCRA, which governs the accuracy, fairness, and privacy of information in the credit files Equifax maintains,

---

30 *Id.* at 4.

31 *Id.* at 3.

32 *Id.* at 10.

33 *Id.*

as well as the GLBA's "rules relating to the physical, administrative and technological protection of non-public personal financial information."[34] Similarly, Equifax recognized that data furnishers and users of credit information, like FI Plaintiffs and the Class, are subject to these same regulations.[35] Equifax also conceded that numerous state data security breach laws "require additional data protection measures which exceed the GLBA data safeguarding requirements," and that "[i]f data within our system is compromised by a breach, we may be subject to provisions of various state security breach laws."[36]

75. Equifax claimed that it devoted "substantial compliance, legal and operational business resources to facilitate compliance with applicable regulations and requirements,"[37] and that it had made a "substantial investment in physical and technological security measures."[38]

76. In its privacy statements, Equifax echoed these promises that it would provide accurate data and that it would adequately safeguard this data. Equifax's summary statement of its privacy policy on its website specifically states: "We have

---

34 *Id.*

35 *Id.*

36 *Id.* at 11.

37 *Id.* at 18.

38 *Id.* at 16.

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. . . . Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax."[39] Equifax's privacy policy further states: "We are committed to protecting the security of your personal information and use technical, administrative and physical security measures that comply with applicable federal and state laws,"[40] and that "[w]e have reasonable physical, technical and procedural safeguards to help protect your personal information."41 [Emphasis added].

77. On another privacy policy webpage, Equifax similarly emphasized that it would "take reasonable steps to . . . [u]se safe and secure systems, including physical, administrative, and technical security procedures to safeguard the information about you." It promoted that it had

---

39 *Privacy*, EQUIFAX INC., https://www.equifax.com/privacy/ (last accessed May 30, 2018).

40 *Equifax Personal Products*, EQUIFAX INC., https://www.equifax.com/privacy/equifax-personal-products/#EffortsWeMakeToSafeguardYourPersonalInformartion (last accessed May 30, 2018).

41 *Personal Credit Reports*, EQUIFAX INC., https://www.equifax.com/privacy/personal-credit-reports/ (last accessed May 30, 2018).

> [S]ecurity protocols and measures in place to protect the personally identifiable information . . . and other information [it] maintain[ed] about you from unauthorized access or alteration. These measures include internal and external firewalls, physical security and technological security measures, and encryption of certain data. When personally identifiable information is disposed of, it is disposed of in a secure manner.[42]

78. In its 2016 Form 10-K, Equifax acknowledged not only its obligation to protect the consumer data it obtains, stores, uses, transmits, sells, and manages, but also the risk that a data breach could occur at Equifax and the impact such a breach would have on Equifax, consumers, and customers:

> ***[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***.
>
> 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, employee or insider error or malfeasance, or other disruptions during the process of upgrading or replacing computer software or hardware, power outages, computer viruses, telecommunication or utility failures or natural

---

[42] *Privacy Policy*, EQUIFAX INC., https://www.equifax.com/cs/Satellite?pagename=privacy_optout (last accessed May 30, 2018).

> disasters or other catastrophic events. ***Unauthorized access to data files or our information technology systems and applications could result in inappropriate use, change or disclosure of sensitive and/or personal data of our customers, employees, consumers and suppliers.***
>
> ***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. Insider or employee cyber and security threats are increasingly a concern for all large companies, including ours. ***Although we are not aware of any material breach of our data, properties, networks or systems, if one or more of such events occur, this potentially could compromise our networks and the information stored there could be accessed, publicly disclosed, lost or stolen. Any such access, disclosure or other loss of information could subject us to litigation, regulatory fines, penalties or reputational damage, any of which could have a material effect on our cash flows, competitive position, financial condition or results of operations***.[43] [Emphasis added].

79. In light of the foregoing statements, Equifax intended FI Plaintiffs and the Class to rely on Equifax to provide accurate data and to adequately safeguard that data. FI Plaintiffs reasonably expected that such information would be stored by Equifax in a safe and confidential manner, using all reasonable safeguards and protections. The potential harm from doing otherwise was obvious to Equifax, which knew that FI Plaintiffs, as payment card issuers, lenders, and deposit account

[43] Equifax Inc., Annual Report (Form 10-K) (Feb. 22, 2017) at 17.

holders, would bear the ultimate responsibility for identity theft and fraudulent lending and other consumer transactions.

80. Equifax explicitly recognized FI Plaintiffs' reliance on the information it provides, stating: "[o]ur products and services enable businesses to make credit and service decisions, manage their portfolio risk, automate or outsource certain payroll-related, tax and human resources businesses processes, and develop certain marketing strategies concerning consumers and commercial enterprises."[44] Equifax also stated: "Businesses rely on us for consumer and business credit intelligence, credit portfolio management, fraud detection, decisioning technology, marketing tools, debit management and human resources-related services."[45]

81. Much like a bailment of personal property, the receipt by Equifax of uniquely-identifying consumer credit-reporting information, PII, and Payment Card Data – for Equifax's own business purposes – places Equifax in a special relationship with FI Plaintiffs and the Class, which rely on Equifax to maintain the security (and hence, the uniquely-identifying nature) of such information. The resulting harm to FI Plaintiffs and Class from mishandling the security and confidentiality of this information was, at all times, foreseeable to Equifax.

---

44 *Id.* at 60.

45 *Id.* at 29.

Equifax Knew that a Breach of Its Computer Systems Was a Foreseeable Risk

82. With data breaches and identity theft on the rise, Equifax undoubtedly knew that a breach of its computer systems was a foreseeable risk. It also knew what the repercussions of such a breach would be.

83. PII and Payment Card Data have considerable value and constitute an enticing and well-known target to hackers. Hackers easily can sell such stolen data as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."[46]

84. The prevalence of data breaches and identity theft has increased dramatically in recent years, accompanied by a parallel and growing economic drain on individuals, businesses, and government entities in the U.S. According to the Identity Theft Resource Center ("ITRC"), in 2017 there were 1,579 reported data breaches in the United States, an all-time high.[47] More than 178.93 million records reportedly were exposed in those breaches (approximately 147.9 million of which

---

[46] Brian Krebs, *The Value of a Hacked Company*, KREBS ON SECURITY (July 14, 2016, 10:47 AM), http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/.

[47] *Data Breach Reports: 2017 End of Year Report*, IDENTITY THEFT RESOURCE CENTER, at 6 (2018), http://www.idtheftcenter.org/images/breach/2017/DataBreachReport_2017.pdf.

were exposed in the Equifax Data Breach alone).[48] The IRTC reported that approximately 60% of the data breaches were the result of hacking.[49]

85. In tandem with the increase in data breaches, the rate of identity theft also reached record levels in 2017, affecting approximately 16.7 million victims in the U.S., with the amount stolen rising to $16.8 billion.[50]

86. Following several high-profile data breaches in recent years, including those involving Target, Experian, Yahoo, Home Depot, and Sony, Equifax was on notice of the very real risk that hackers could exploit vulnerabilities in its data security.

87. These and other data breaches have been well publicized. Unfortunately, Equifax did not view these breaches as cautionary tales, but rather as another avenue to profit from businesses and consumers concerned with fraud. Equifax's CEO Richard Smith admitted as much in an August 2017 speech where

---

48 *Id.*

49 *Id.* at 4.

50 Press Release, Javelin Strategy & Research, *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study* (Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin.

he referred to consumer fraud as a "huge opportunity" and "massive, growing business" for Equifax.[51]

Equifax Knew What the Repercussions of a Data Breach Would Be

88. As evidenced by its own product offerings, Equifax held itself out as a leader and expert in anticipating and combatting cybersecurity threats. In marketing these solutions, data security was Equifax's sales pitch.[52]

89. Equifax even developed and sold "data breach solutions" to financial institutions, like FI Plaintiffs and the Class, to combat the "great risk of identity theft and fraud."

90. Equifax maintains a dedicated landing page to sell products and services: https://www.equifax.com/help/data-breach-solutions.

---

[51] Jim Puzzanghera, *Senators Slam Equifax for making money off massive data breach and no-bid IRS contract*, LOS ANGELES TIMES (Oct. 4, 2017), http://www.latimes.com/business/la-fi-equifax-senate-20171004-story.html; Megan Leonhardt, *Equifax Is Going to Make Millions Off Its Own Data Breach*, TIME (Oct. 4, 2017), http://time.com/money/4969163/equifax-hearing-elizabeth-warren-richard-smith/.

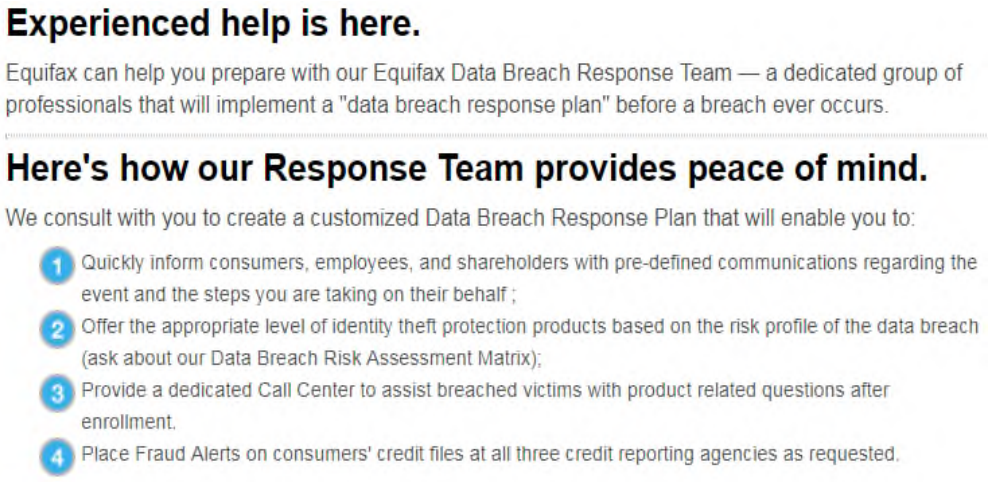
[52] Stacy Cowley & Tara Siegel Bernard, *As Equifax Amassed Ever More Data, Safety Was a Sales Pitch*, NEW YORK TIMES (Sept. 23, 2017), https://www.nytimes.com/2017/09/23/business/equifax-data-breach.html.

91. In its marketing materials, Equifax states: "You'll feel safer with Equifax. We're the leading provider of data breach services, serving more than 500 organizations with security breach events every day. In addition to extensive experience, Equifax has the most comprehensive set of identity theft products and customer service coverage in the market."[53]

92. Equifax also has touted its "Data Breach Response Team," which includes a "dedicated group of professionals that will implement a 'data breach response plan' before a breach ever occurs," including informing "consumers, employees, and shareholders with pre-defined communications" regarding the

53 *Equifax Data Breach Solutions*, EQUIFAX INC., https://www.equifax.com/help/data-breach-solutions (last accessed May 30, 2018).

breach, offering identity theft protection products, providing a dedicated call center to assist breach victims, and placing fraud alerts on consumers' credit files.[54]



Experienced help is here.

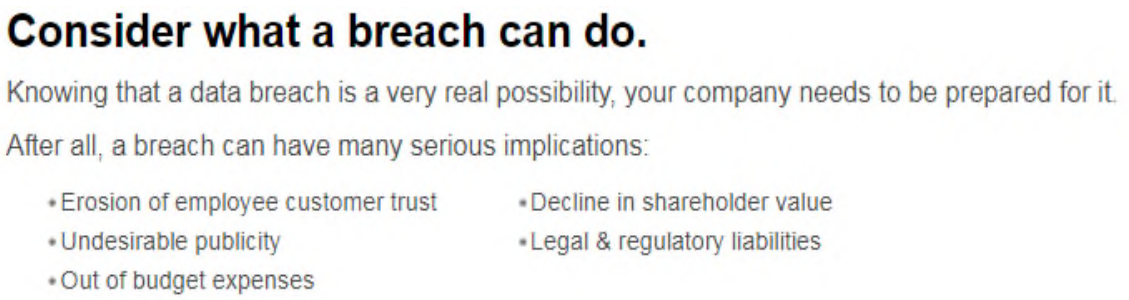
Equifax can help you prepare with our Equifax Data Breach Response Team — a dedicated group of professionals that will implement a "data breach response plan" before a breach ever occurs.

Here's how our Response Team provides peace of mind.

We consult with you to create a customized Data Breach Response Plan that will enable you to:

1. Quickly inform consumers, employees, and shareholders with pre-defined communications regarding the event and the steps you are taking on their behalf ;
2. Offer the appropriate level of identity theft protection products based on the risk profile of the data breach (ask about our Data Breach Risk Assessment Matrix);
3. Provide a dedicated Call Center to assist breached victims with product related questions after enrollment.
4. Place Fraud Alerts on consumers' credit files at all three credit reporting agencies as requested.

93. Equifax even summarized some of the repercussions of a data breach, including the erosion of employee and customer trust, decline in shareholder value, undesirable publicity, legal and regulatory liabilities, and out of budget expenses. Equifax, therefore, fully understood the consequences of failing to secure its data.[55]



Consider what a breach can do.

Knowing that a data breach is a very real possibility, your company needs to be prepared for it. After all, a breach can have many serious implications:

- Erosion of employee customer trust
- Undesirable publicity
- Out of budget expenses
- Decline in shareholder value
- Legal & regulatory liabilities

54 *Id.*

55 *Id.*

94. In 2017, Equifax's Chief Information Security Officer ("CISO"), Susan Mauldin, was interviewed about "how the role of a Chief Information Security Officer has evolved in response to growing cybersecurity threats."[56] In the interview, Ms. Mauldin discussed at length her methods for addressing expected cybersecurity threats, stating: "We spend our time looking for threats against a company. We look for things that might be active inside the company that would cause us concern, and then of course we look to respond – detecting, containing and deflecting those threats."[57] She went on to outline some of her "best practices" for combatting cybersecurity threats. It was later revealed that Ms. Mauldin had no formal training in information systems or cybersecurity; rather, her training was in music composition.

95. Thus, Equifax knew, given the vast amount of PII it managed, that it was a "regular" target of attempted cyber and other security threats and therefore understood the risks posed by its insecure and vulnerable computer systems and website. It also understood the need to safeguard PII and the impact a data breach would have on financial institutions, including FI Plaintiffs and the Class.

---

56 Prat Moghe, *Interview with Equifax CISO Susan Mauldin*, CAZENA, https://web.archive.org/web/20170908175854/https:/www.cazena.com/susan-mauldin-transcript (last visited May 29, 2018).

57 *Id.*

Equifax Knew that Its Data Security Practices Were Inadequate

96. Equifax has a long history of maintaining data security measures that are inadequate for the scale and complexity of its business and the sensitivity of the consumer data that it obtains, stores, uses, transmits, sells, and manages. In the months leading up to the Data Breach, Equifax experienced multiple security breaches, where consumer PII was compromised as a result of deficient data security measures. Therefore, Equifax knew that its data security practices were inadequate.

97. For instance, in March 2015, Equifax admitted "that it mistakenly exposed consumer data as a result of a technical error that occurred during a software change."[58] Equifax inadvertently mailed credit report information, including Social Security numbers and sensitive account information, to unauthorized individuals who did not request the information.[59] A woman in Maine received from Equifax

---

[58] Office of Sen. Elizabeth Warren, *Bad Credit: Uncovering Equifax's Failure to Protect American's Personal Information*, at 4 (Feb. 2018), https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf [hereinafter Warren Report]; *see also Emails Reveal New Details About Equifax Data Breach, AG Announces Settlement*, CBS 13 & BANGOR DAILY NEWS (May 30, 2015), https://bangordailynews.com/2015/05/30/news/state/emails-reveal-new-details-about-equifax-data-breach-ag-announces-settlement/ [hereinafter CBS 13 & BANGOR DAILY NEWS, *Emails Reveal New Details*].

[59] *Equifax Discloses Data Breach Due to Technical Error During Software Change*, DATABREACHES.NET (April 9, 2015),

hundreds of credit reports belonging to others.[60] Equifax later informed the Maine Bureau of Consumer Credit Protection that a software upgrade error led to the mailing of the credit reports to the wrong individuals.[61]

98. In April 2016, Equifax's W-2Express website (http://w2express.com), which allowed employees to access copies of their W-2 tax forms, suffered a data breach in which hackers accessed the salary and tax information of more than 800 current and former employees of Stanford University and Northwestern University through the W-2Express website.[62]

---

https://www.databreaches.net/equifax-discloses-data-breach-due-to-technical-error-during-software-change/.

60 John Chrisos, *Credit Agency Mistakenly Sends 300 Confidential Reports to Maine Woman*, CBS 13 & BANGOR DAILY NEWS (March 19, 2015), http://bangordailynews.com/2015/03/19/news/state/credit-agency-mistakenly-sends-300-confidential-reports-to-maine-woman/.

61 CBS 13 & Bangor Daily News, *Emails Reveal New Details*, *supra* n.58.

62 Hannah Knowles, *University Employees Vulnerable After Tax Data Breach*, STANFORD DAILY (April 12, 2016), https://www.stanforddaily.com/2016/04/12/university-employees-vulnerable-after-tax-data-breach/; *see also Northwestern University Announcement, Update on IRS Tax Filings and W-2 Access*, NORTHWESTERN UNIVERSITY (April 22, 2016), https://news.northwestern.edu/stories/2016/04/update-on-irs-tax-filings-and-w-2-access/; Peter Kotecki, *Tax Fraud, Identity Theft Affect More Than 250 Northwestern Employees*, DAILY NORTHWESTERN (April 27, 2016), https://dailynorthwestern.com/2016/04/27/campus/tax-fraud-identity-theft-affect-more-than-250-northwestern-employees/; Lisa M. Krieger, *Some Stanford Employees Are Victims of Social Security Fraud*, MERCURY NEWS (Aug. 25, 2017),

99. Similarly, in May 2016, Equifax's W-2Express website was breached again, resulting in the disclosure of 430,000 names, addresses, Social Security numbers, and other personal information of current and past employees of grocery retail giant Kroger.[63] The W-2Express website breach occurred because Equifax used weak default login information based on users' partial Social Security number and year of birth, information easily obtained by third parties.[64]

100. Then, between April 2016 and March 2017, TALX Corp., an Equifax subsidiary now referred to as Equifax Workforce Solutions that provides online payroll, HR, and tax services, suffered a data breach where hackers stole Equifax

https://www.mercurynews.com/2017/08/25/stanford-victims-of-social-security-fraud/.

63 Warren Report, *supra* n.58; *see also* Thomas Fox-Brewster, *A Brief History of Equifax Security Fails*, FORBES (Sept. 8, 2017), https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#2661e102677c; Brian Krebs, *Crooks Grab W-2s from Credit Bureau Equifax*, KREBS ON SECURITY (May 6, 2016), https://krebsonsecurity.com/2016/05/crooks-grab-w-2s-from-credit-bureau-equifax.

64 Jeremy Henley, *The Kroger/Equifax W-2 Breach: What Can We Learn From It*, IDEXPERTS.COM (June 7, 2016), https://www2.idexpertscorp.com/knowledge-center/single/the-kroger-equifax-w-2-breach-what-can-we-learn-from-it.

customers' employees' W-2 tax data by resetting the employees' 4-digit PIN password after answering personal identifying questions about those employees.[65]

101. In January 2017, a LifeLock customer was able to view several unrelated persons' credit reports through the LifeLock online portal. Equifax researched the issue and acknowledged that credit information of a "small number of LifeLock members" was inadvertently sent to another member's online portal "as the result of a technical issue."[66]

102. In light of the foregoing breaches of Equifax's systems, Equifax knew that its data security practices were inadequate. Equifax also knew or should have known of its many security deficiencies from the criticisms levied by multiple third parties that concluded Equifax was highly susceptible to a data breach.

---

65 Brian Krebs, *Fraudsters Exploited Lax Security at Equifax's TALX Payroll Division*, KREBS ON SECURITY (May 18, 2017), https://krebsonsecurity.com/2017/05/fraudsters-exploited-lax-security-at-equifaxs-talx-payroll-division/.

66 Letter from King & Spalding LLP to Attorney General Joseph Foster Regarding Data Incident Notification (Feb. 8, 2017), https://www.doj.nh.gov/consumer/security-breaches/documents/equifax-20170208.pdf.

103. In August 2016, MSCI, Inc. ("MSCI"), an institutional investor research analyst, criticized "Equifax Inc.'s poor data security and privacy measures" and downgraded Equifax to "CCC," MSCI's lowest possible rating.[67]

104. In December 2016, MSCI issued a follow-up research report and stated: "Equifax is vulnerable to data theft and security breaches, as is evident from the 2016 breach of 431,000 employees' salary and tax data of one of its largest customers, Kroger grocery chain. The company's data and privacy policies are limited in scope and Equifax shows no evidence of data breach plans or regular audits of its information security policies and systems."[68]

105. Also in December 2016, a security researcher warned Equifax that one of Equifax's public-facing websites "displayed several search fields, and anyone – with no authentication whatsoever – could force the site to display the personal data of Equifax's customers."[69] The flaw was discovered on a webpage that appeared to

---

67 *MSCI ESG Ratings May Help Identify Warning Signs*, MSCI, at 1, https://www.msci.com/documents/1296102/6174917/MSCI-ESG-Ratings-Equifax.pdf/b95045f2-5470-bd51-8844-717dab9808b9 (last visited May 30, 2018).

68 *Id.*

69 Lorenzo Franceschi-Bicchierai, *Equifax Was Warned*, VICE (Oct. 26, 2017), https://motherboard.vice.com/en_us/article/ne3bv7/equifax-breach-social-securitynumbers-researcher-warning.

be a portal for Equifax employees, but was open to anyone on the internet.[70] The researcher accessed full names, Social Security numbers, birth dates, and city and state of residence information for "every American" through Equifax's unsecured website.[71] The researcher also took control of several Equifax servers and found that the servers were running outdated software vulnerable to further breaches. The researcher immediately reported the security flaw to Equifax and stated: "[i]t should've been fixed the moment it was found. It would have taken them five minutes, they could've just taken the site down."[72] Instead, it took Equifax six months to patch that vulnerability.[73]

106. In addition, four independent analyses of Equifax's systems and controls relating to cybersecurity – conducted either before or immediately after the Data Breach – identified serious weaknesses, including that Equifax "was behind on basic maintenance of websites that could have been involved in transmitting

---

70 *Id.*

71 *Id.*

72 *Id.*

73 *Id.*; *see also* George Cox, *Equifax Suffers Another Security Breach*, THE SPECTRUM (Nov. 8, 2017), https://www.thespectrum.com/story/life/features/mesquite/2017/11/08/equifaxsuffers-another-security-breach/842717001/.

sensitive consumer information and scored poorly in areas" highly susceptible to data breaches.[74]

107. In April 2017 – the month before the Data Breach – Cyence, a cyber-risk analysis firm, "rated the danger of a data breach at Equifax during the next 12 months at 50%. It also found the company performed poorly when compared with other financial-services companies."[75]

108. SecurityScorecard, another security monitoring firm, identified the precise weakness that was used by the hackers to breach the Equifax system, reporting that "Equifax used older software – such as the Apache Struts tool kit . . . and often seemed slow to install patches."[76]

109. An outside review by Fair Isaac Corporation ("FICO") rated Equifax's "enterprise security score" based on three elements: hardware, network security, and web services. The score declined from 550 out of 800 at the beginning of 2017 to 475 in mid-July 2017. The FICO analysis found that public-facing websites run by

---

74 AnnaMaria Andriotis & Robert McMillan, *Equifax Security Showed Signs of Trouble Months Before Hack*, THE WALL STREET JOURNAL (Sept. 26, 2017), https://www.wsj.com/articles/equifax-security-showed-signs-of-trouble-months-before-hack-1506437947.

75 Warren Report, *supra* n.58, at 5.

76 *Id.*

Equifax used expired security certificates and had errors in the chain of certificates and other web-security issues. Updated security certificates are vital to data security because they are used to authenticate the connection between a user's web browser and an HTTPS web server, allowing the user to know that its connection to a website is legitimate and secure.[77]

110. A fourth independent review – released just after the Equifax Data Breach was announced – also identified significant problems with Equifax cybersecurity. This BitSight Technologies report gave Equifax an "F" in application security and a "D" for software patching.[78]

111. These criticisms underscored Equifax's own awareness that it was highly susceptible to a data breach.

Equifax Ignored the Notification of the Specific Vulnerability That Led to the Data Breach

112. On September 7, 2017, Equifax announced that between May 13, 2017 and July 30, 2017, hackers exploited a vulnerability in Equifax's U.S. web server software to gain access to the PII of approximately 143 million U.S. consumers and

77 *Id.*

78 *Id.*

the Payment Card Data of 209,000 cardholders.[79] The estimated number of U.S. consumers impacted by the Data Breach later was increased to 147.9 million.[80]

113. The attack vector used in this incident occurred through vulnerabilities in Apache Struts (CVE-2017-5638), an open-source application framework that supports the Equifax online dispute portal web application.[81]

114. Equifax's online dispute portal, which is located at https://www.equifax.com/personal/disputes/, allows consumers to dispute inaccurate information contained on their credit files.

115. To access the online dispute portal, a user must input certain PII, including name, address, Social Security number, date of birth, and email address, along with an optional ten digit confirmation code, which is the confirmation number

---

79 *Equifax Announces Cybersecurity Incident Involving Consumer Information*, EQUIFAX INC., (Sept. 7, 2017), https://investor.equifax.com/news-and-events/news/2017/09-07-2017-213000628.

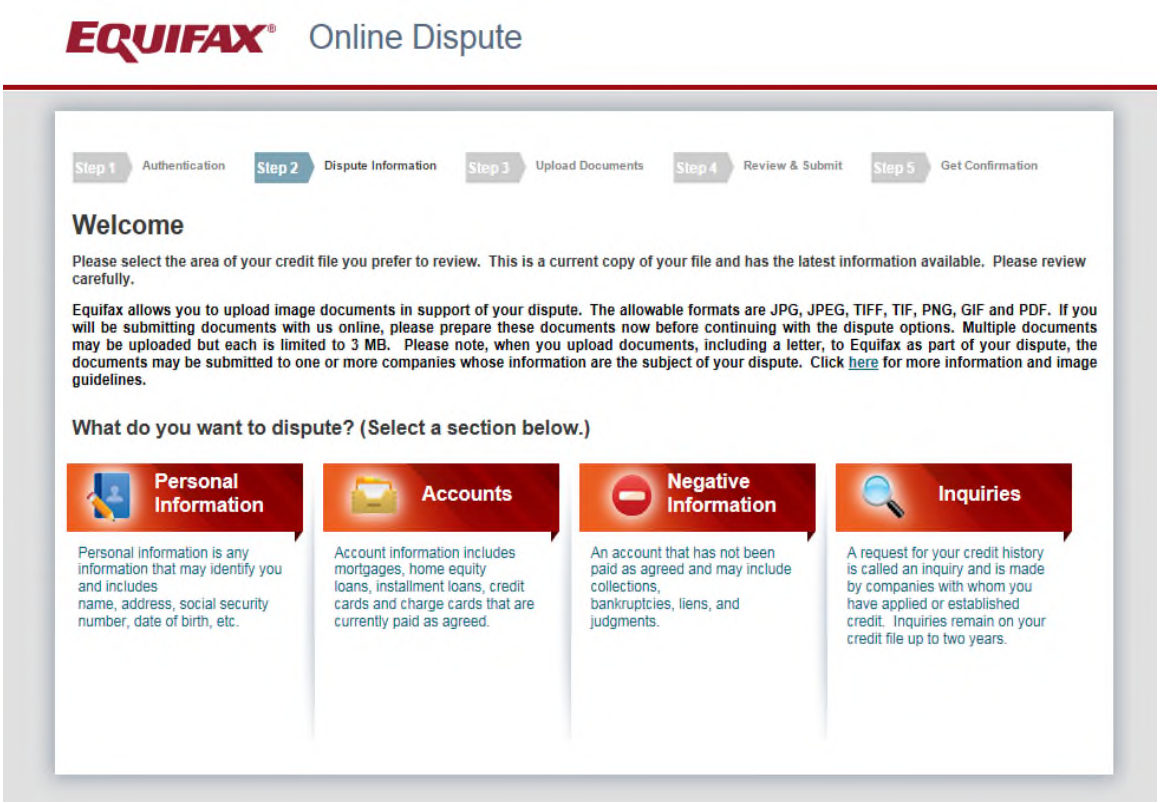
80 AnnaMaria Andriotis, *Equifax Identifies Additional 2.4 Million Affected by 2017 Breach*, THE WALL STREET JOURNAL (March 1, 2018), https://www.wsj.com/articles/equifax-identifies-additional-2-4-million-affected-by-2017-breach-1519918282.

81 *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, EQUIFAX INC., (Sept. 15, 2017), https://www.equifaxsecurity2017.com/2017/09/15/equifax-releases-details-cybersecurity-incident-announces-personnel-changes/.

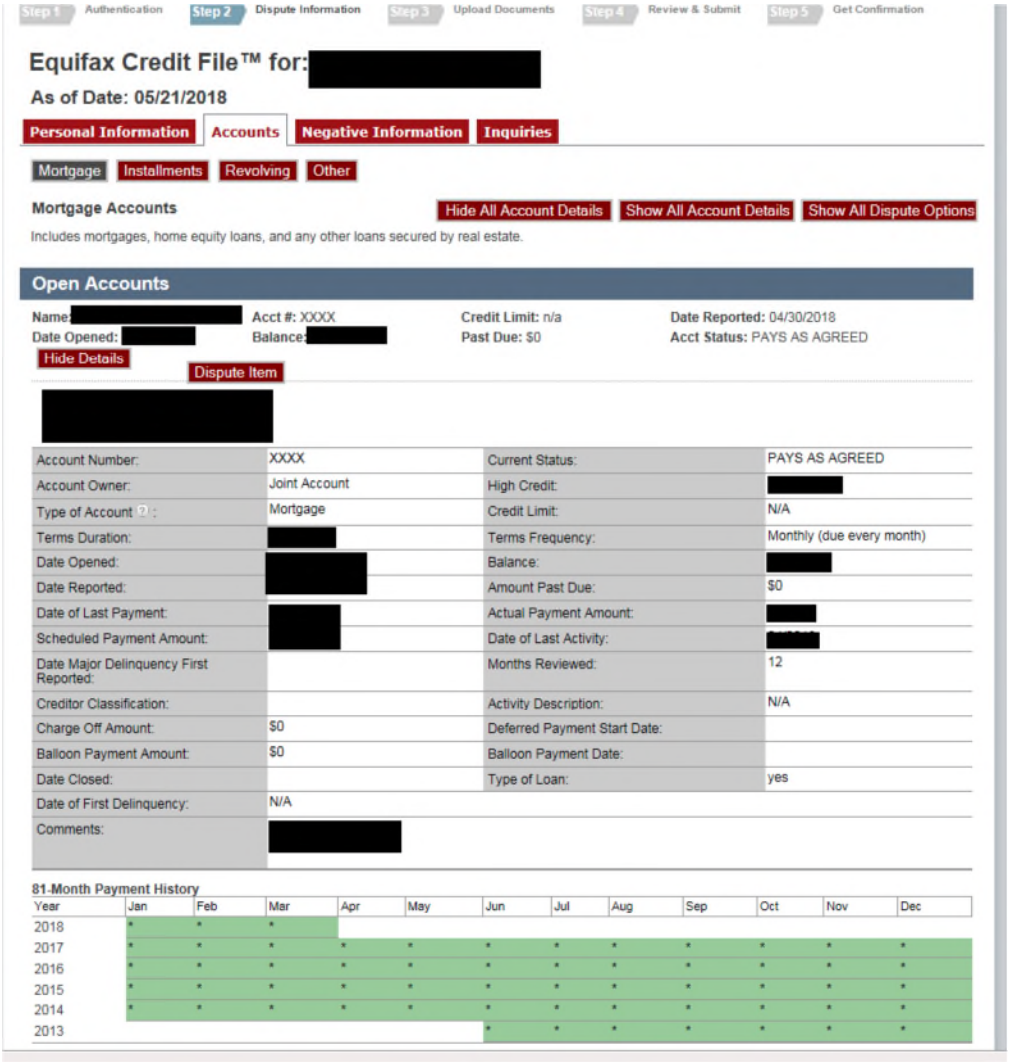
found on the copy of a customer's credit file, or the confirmation number provided by Equifax when the customer created the online dispute.

116. Once a user provides the requested PII, they are able to review information regarding their credit, including their personal information (such as name, address, Social Security number, date of birth), credit history for their accounts (for credit products such as mortgages, loans, and credit cards), amounts

owed for each credit product, and any negative information regarding their credit (late payments, collection information, and bankruptcy filings).



117. As the following images show, all the data contained in the credit file is available once the dispute resolution portal is accessed:



Step 1 Authentication Step 2 Dispute Information Step 3 Upload Documents Step 4 Review & Submit Step 5 Get Confirmation

Equifax Credit File™ for: [redacted]

As of Date: 05/21/2018

Personal Information | Accounts | Negative Information | Inquiries

Mortgage | Installments | Revolving | Other

Mortgage Accounts Hide All Account Details | Show All Account Details | Show All Dispute Options

Includes mortgages, home equity loans, and any other loans secured by real estate.

Open Accounts

Name: [redacted] Acct #: XXXX Credit Limit: n/a Date Reported: 04/30/2018
Date Opened: [redacted] Balance: [redacted] Past Due: $0 Acct Status: PAYS AS AGREED

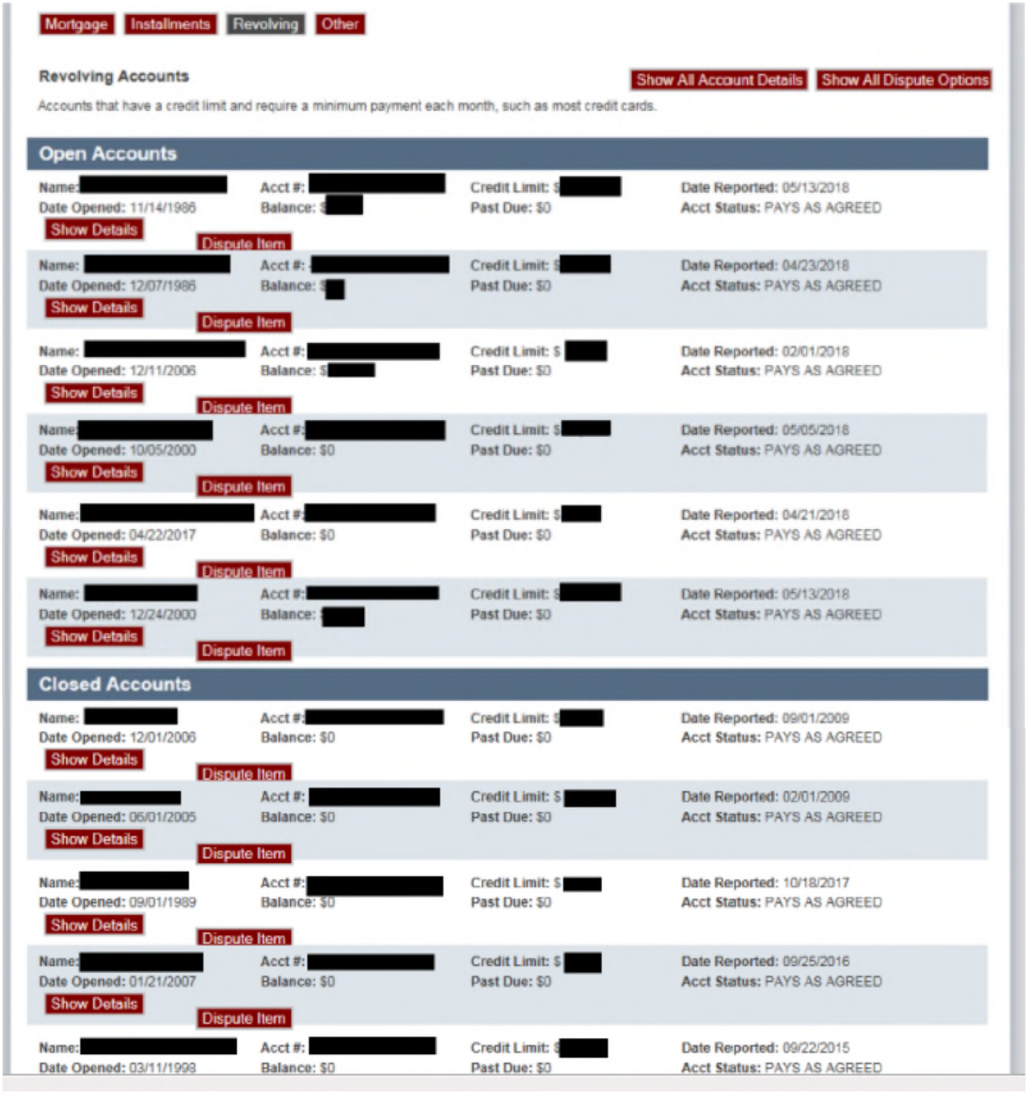
Hide Details Dispute Item

[redacted]

Account Number:	XXXX	Current Status:	PAYS AS AGREED
Account Owner:	Joint Account	High Credit:	[redacted]
Type of Account ? :	Mortgage	Credit Limit:	N/A
Terms Duration:	[redacted]	Terms Frequency:	Monthly (due every month)
Date Opened:	[redacted]	Balance:	[redacted]
Date Reported:		Amount Past Due:	$0
Date of Last Payment:	[redacted]	Actual Payment Amount:	[redacted]
Scheduled Payment Amount:		Date of Last Activity:	[redacted]
Date Major Delinquency First Reported:		Months Reviewed:	12
Creditor Classification:		Activity Description:	N/A
Charge Off Amount:	$0	Deferred Payment Start Date:	
Balloon Payment Amount:	$0	Balloon Payment Date:	
Date Closed:		Type of Loan:	yes
Date of First Delinquency:	N/A		
Comments:	[redacted]		

81-Month Payment History

Year	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
2018	*	*	*									
2017	*	*	*	*	*	*	*	*	*	*	*	*
2016	*	*	*	*	*	*	*	*	*	*	*	*
2015	*	*	*	*	*	*	*	*	*	*	*	*
2014	*	*	*	*	*	*	*	*	*	*	*	*
2013						*	*	*	*	*	*	*



118. Equifax represents that the credit information provided through the online dispute portal is "a current copy of your file and has the latest information available." In other words, the ***full content*** of a consumer's credit file, including ***all the consumer data that financial institutions furnish to Equifax***, is available once the online dispute portal is accessed. By entering through the dispute resolution portal, it is possible that the hacker had access to consumers' complete credit files.

119. The dispute resolution portal website runs on Apache Struts software, a popular programming framework for building web applications in Java. Apache Struts makes it "easier for developers to build top-to-bottom custom websites" and it "can handle everything from interactive screens and logins, to web apps and database management."[82] Apache Struts is "open source," meaning that the source code is made freely available and may be redistributed and modified by anyone who wants to use it.

120. While Apache Struts has been widely used by companies and government agencies for years, and is currently in use by at least 65% of Fortune 100 companies,[83] its popularity and expansive capabilities leave it vulnerable to cyberattacks. Indeed, because the software "touches all aspects of a company's website," once hackers locate a vulnerability, they gain "unfettered access" to the

---

82 Ben Popken, *Equifax Hackers Exploited Months-Old Flaw*, NBC NEWS (Sept. 14, 2017), https://www.nbcnews.com/business/consumer/how-did-equifax-hackeven-happen-n801331.

83 Keith Collins, *The Hackers Who Broke into Equifax Exploited a Flaw in Opensource Server Software*, QUARTZ (Sept. 8, 2017), https://qz.com/1073221/thehackers-who-broke-into-equifax-exploited-a-nine-year-old-security-flaw/.

underlying system and can "execute commands just like they were the administrators." In other words, "they basically control the system."[84]

121. According to a report in the *Wall Street Journal*, the vulnerability in Apache Struts "would allow hackers to break into a company by sending data to a server that was specially crafted to take advantage of the flaw. It was the digital equivalent of popping open a side window to sneak into a building."[85]

122. Once discovered, the potential vulnerability of the Apache Struts software was widely announced so that users of the software could remediate the vulnerability. In March 2017, several entities, including The Apache Foundation, the U.S. Department of Commerce's National Institute of Standards and Technology ("NIST"), and the U.S. Department of Homeland Security's Computer Emergency Readiness Team ("U.S. CERT"), issued public warnings regarding the vulnerability. The Apache Foundation and NIST described the flaw as "critical," which is the highest rating those groups use to indicate the danger of a vulnerability.

---

84 *See* Popken, *supra* n.82.

85 Andriotis *et al.*, '*We've Been Breached*': *Inside the Equifax Hack*, *supra* n.3.

123. On March 7, 2017, the same day the vulnerability was publicly announced, The Apache Foundation also made available various patches and workarounds to protect against the vulnerability.[86]

124. After this vulnerability was publicly identified, media reports indicated that hackers already were exploiting the vulnerability against various companies and government agencies.[87]

125. Equifax publicly stated that its security team "was aware of this vulnerability [with Apache Struts] at that time [in March 2017]."[88] On March 8, 2017, U.S. CERT sent Equifax a notice of the need to patch a particular vulnerability in the "Apache Struts" software.[89] Equifax admitted that it received the U.S. CERT notification and disseminated it on March 9, 2017.[90]

---

86 Elizabeth Weise & Nathan Borney, *Equifax Had Patch 2 Months Before Hack and Didn't Install It, Security Group Says*, USA TODAY (Sept. 14, 2017), https://www.usatoday.com/story/money/2017/09/14/equifax-identity-theft-hackers-apache-struts/665100001/.

87 Dan Goodin, *Critical Vulnerability Under "Massive" Attack Imperils High-impact Sites*, ARSTECHNICA (Mar. 9, 2017), https://arstechnica.com/information-technology/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites/.

88 *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, *supra* n.81.

89 *Smith Testimony*, *supra* n.1, at 2–3.

90 *Id.*

126. Equifax even knew that patches for the vulnerability were available, but Equifax senior management decided not to implement the patch and instead affirmatively decided to continue to use the outdated version of the software for two and a half months without applying the available patches or taking other measures to protect against the flaw.[91]

127. Equifax admits that it ran security scans on March 15, 2017, that could have alerted Equifax to the Apache Struts vulnerability. However, because certain key systems did not have proper security certificates, Equifax failed to scan all of its systems and therefore did not discover the Apache Struts vulnerability.[92]

---

[91] George Leopold, *Equifax Ignored Apache Struts Patch For Months*, ENTERPRISETECH (Sept. 15, 2017), https://www.enterprisetech.com/2017/09/15/equifax-ignored-apache-struts-patch-months/; *see also The Apache Software Foundation, MEDIA ALERT: The Apache Software Foundation Confirms Equifax Data Breach Due to Failure to Install Patches Provided for Apache® Struts™ Exploit*, THE APACHE SOFTWARE FOUNDATION BLOG (Sept. 14, 2017), *https://blogs.apache.org/foundation/entry/media-alert-the-apache-softwarez* [hereinafter The Apache Software Foundation, MEDIA ALERT].

[92] Equifax: Continuing to Monitor Data-Broker Cybersecurity: Hearing Before the SubComm. On Privacy, Technology and the Law of the S. Comm. On the Judiciary, 115th Cong. (2017), (Equifax's Submission in Response to Subcommittee's Requests Dated October 11, 2017), https://www.judiciary.senate.gov/imo/media/doc/Smith%20Responses%20to%20QFRs2.pdf [hereinafter Equifax's Oct. 11, 2017 Responses].

128. Security certificates are designed to secure data that is transmitted between two systems through the use of encryption. There are two main protocols for security certificates, Secure Socket Layer ("SSL") and Transport Layer Security ("TLS"). Both SSL and TLS allow systems to transmit encrypted information, authenticate that the system is what it claims to be (as opposed to being a server or system used by a malicious third party), and ensure that the systems are communicating with known and authenticated systems. Software tools that scan systems and applications to identify vulnerabilities cannot work on web portals with expired security certificates.[93] Therefore, because Equifax did not properly update its security certifications and allowed its security certificates to expire, Equifax's scans failed to identify the Apache Struts vulnerability.

129. Equifax admits that its systems were breached on May 13, 2017, well over two months after Equifax should have patched the Apache Struts

[93] For example, Symantec offers as part of its security certificates free malware scanning to detect potential vulnerabilities. *See Malware Scanning*, Symantec, https://www.websecurity.symantec.com/security-topics/malware-scanning (last accessed May 30, 2018).

vulnerability.[94] Equifax also acknowledges the unpatched vulnerability in the Apache Struts software allowed hackers to access PII.[95]

130. Between May 13 and July 30, 2017, hackers utilized simple commands to identify the credentials of network accounts at Equifax, allowing them to traverse multiple databases to access and infiltrate the sensitive personal information, including names, Social Security numbers, birth dates, addresses, and driver's license numbers, of approximately 147.9 million U.S. consumers.[96]

131. Indeed, shortly after Equifax publicly announced the Data Breach at issue, security researchers discovered that one of Equifax's online employee portals could be accessed by using the word "admin" for both the login and password. Once

---

94 *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, *supra* n.81.

95 *Smith Testimony*, *supra* n.1, at 2–3.

96 AnnaMaria Andriotis & Robert McMillan, *Hackers Entered Equifax Systems in March*, THE WALL STREET JOURNAL (Sept. 20, 2017), https://www.wsj.com/articles/hackers-entered-equifax-systems-in-march-1505943617; Andriotis, *Equifax Identifies Additional 2.4 Million Affected by 2017 Breach*, *supra* n.80.

logged in through the portal, a hacker could easily access sensitive employee and consumer data.[97]

132. In addition to compromising the PII, the hackers accessed 209,000 consumer credit card numbers, and an estimated 182,000 dispute records containing additional personal information.[98] Equifax stated that it believes all consumer credit card numbers were accessed in one fell swoop in mid-May 2017.

133. On September 11, 2017, Visa issued a CAMS alert of a potential network intrusion at Equifax that put Visa accounts at risk. The Visa CAMS alert indicated that the exposure window was approximately November 10, 2016 through July 6, 2017 and that the debit and credit card data compromised included PAN, CVV2, expiration dates, and cardholder names. Visa further stated that financial institutions receiving the CAMS alert should take necessary steps to prevent fraud and safeguard cardholders.

134. On September 11, 2017, MasterCard issued an ADC alert of a potential network intrusion at Equifax that put MasterCard accounts at risk. The MasterCard ADC alert indicated that the exposure window was approximately November 10,

---

97 *See* Brian Krebs, *Ayuda! (Help!) Equifax Has My Data!*, KREBS ON SECURITY (Sept. 17, 2017), https://krebsonsecurity.com/2017/09/ayuda-help-equifax-has-my-data/.

98 Equifax Inc., Annual Report (Form 10-K) (Mar. 1, 2018) at 2 & 34.

2016 through July 6, 2017 and that the debit and credit card data compromised included account number and expiration date.

135. In a statement posted September 14, 2017, The Apache Software Foundation attributed the Equifax Data Breach to a single cause: Equifax's "failure to install the security updates provided in a timely manner,"[99] despite being notified about the vulnerabilities in Apache Struts.

136. On October 2, 2017, Equifax announced that Mandiant had completed its internal forensic analysis of the Data Breach. Mandiant determined that an additional 2.5 million consumer records may have been compromised, bringing the total number of potentially compromised accounts to 145.5 million.

137. On November 7, 2017, Visa issued an updated CAMS alert stating that the exposure window had been expanded to August 20, 2016 through July 6, 2017. The updated alert identified the debit and credit card data compromised as PAN, expiration date, cardholder name, cardholder address, Social Security number, and cardholder zip code.

138. On November 20, 2017, MasterCard issued an updated ADC alert. The updated alert indicated that the exposure window was approximately August 10,

[99] The Apache Software Foundation, MEDIA ALERT, *supra* n.91.

2016 through September 8, 2017 and that the compromised debit and credit card data included account number, expiration date, Social Security number or equivalent cardholder name and cardholder address.

139. On March 1, 2018, Equifax announced that 2.4 million more U.S. consumers were impacted by the Data Breach than previously disclosed, bringing the total number of potentially compromised accounts to 147.9 million.[100] These additional consumers had names and partial driver's license numbers stolen, according to reports.[101]

140. On May 7, 2018, Equifax submitted a "statement for the record" to the SEC more fully detailing the breakdown of stolen PII.[102]

Information Stolen	Approximate Number of Impacted U.S. Customers
Name	146.6 million
Date of Birth	146.6 million
Social Security Number	145.5 million
Address Information	99 million
Gender	27.3 million
Phone Number	20.3 million

100 Andriotis, *Equifax Identifies Additional 2.4 Million Affected by 2017 Breach*, *supra* n.80.

101 *Id.*

102 Equifax Inc., 2016 Form 8-K (May 7, 2018) at 2.

Driver's License Number	17.6 million
Email Address	1.8 million
Payment Card Number and Expiration Date	209,000
Tax ID	97,500
Driver's License State	27,000

141. Equifax also reported that, in addition to the PII that was previously identified as stolen in the Data Breach, customers' passports, taxpayer identification cards, state identification cards, resident alien cards, and military identification cards were also stolen.[103] These items were required by Equifax and were provided by customers who submitted scans of their ID cards to verify their identity in connection with the online dispute portal.[104]

Equifax Delayed Publicly Announcing the Data Breach

142. Equifax reportedly discovered this Data Breach on July 29, 2017, over four and a half months after U.S. CERT issued a notification about the Apache Struts

103 *Id.* at 3.

104 *Id.*

vulnerability, when Equifax's security team noticed "suspicious network traffic" connected to its consumer dispute portal website.[105]

143. Equifax's security department continued investigating the abnormal activity and, on July 30, 2017, determined that the intrusion was serious enough that the consumer dispute portal website needed to be taken entirely offline.[106]

144. Equifax's CEO Richard Smith was informed of the Data Breach the following day, on July 31, 2017.[107]

145. While Equifax would not disclose the Data Breach to the public for several more weeks, Equifax senior management profited, selling stock or exercising options worth $2.7 million. On August 1, 2017, only three days after Equifax discovered the Data Breach, Equifax Chief Financial Officer John Gamble sold $946,374 worth of stock, and President of U.S. Information Solutions Joseph Loughran exercised options to sell $584,099 worth of stock. The next day, President of Workforce Solutions Rodolfo Ploder sold $250,458 worth of stock, and Chief

---

105 *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, *supra* n.81.

106 *Id.*

107 *Smith Testimony*, *supra* n.1, at 3.

Information Officer Jun Ying sold $950,000 worth of stock.[108] None of those transactions were part of previously scheduled Rule 10b5-1 trading plans.

146. On August 2, 2017, Equifax informed the Federal Bureau of Investigation ("FBI") about the Data Breach and retained the law firm of King & Spalding LLP to guide its investigation of the Data Breach. Equifax also hired the cybersecurity forensic firm Mandiant to analyze and investigate the suspicious activity on its network.

147. Over the next several weeks, Mandiant and Equifax's internal security department analyzed forensic data to determine the nature and scope of the suspicious activity. The investigators determined that Equifax had been subject to cyber-intrusions that resulted in a breach of Equifax's IT systems.

148. Equifax did not notify its chairman of its board of directors about the Data Breach until August 22, 2017, and waited two more days to inform the full board of directors.

149. Equifax finally publicly revealed the Data Breach on September 7, 2017. But not only did Equifax delay its public announcement for forty days after

---

[108] Anders Melin, *Three Equifax Managers Sold Stock Before Cyber Hack Revealed*, BLOOMBERG.COM (Sept. 7, 2017), https://www.bloomberg.com/news/articles/2017-09-07/three-equifaxexecutives-sold-stock-before-revealing-cyber-hack.

it learned of the Data Breach, it also soundly botched the next steps in its breach response program.

150. To handle consumer inquiries after the public announcement, Equifax created a website, https://www.equifaxsecurity2017.com/, to enable consumers to determine whether they were potentially impacted by the Data Breach. In order to determine whether they were affected, Equifax required consumers to provide their last names and the last six digits of their Social Security numbers. In essence, Equifax required customers potentially harmed by the Data Breach to provide Equifax with additional sensitive information in order to determine whether their already-provided sensitive information was stolen through the Data Breach.

151. After consumers provided their sensitive information, Equifax's website displayed whether the inquirer was impacted. Under the notice, Equifax's webpage directed consumers to a free identity theft protection and credit monitoring program, TrustedID (a wholly owned subsidiary of Equifax). Equifax offered the identity theft protection and credit monitoring services in the wake of the Data Breach. However, by signing up for TrustedID, consumers consented, often unknowingly, to settle all claims arising out of the use of TrustedID in arbitration. After public outrage over the waiver, Equifax claimed its waiver did not extend to harm caused by the Data Breach.

152. After permitting what is likely to be one of the most damaging data breaches in history, Equifax continued to severely mismanage its websites. Starting on September 9, 2017, Equifax erroneously directed consumers to a fake website at least four times via Twitter.[109] Rather than directing consumers to https://www.equifaxsecurity2017.com/ (Equifax's legitimate website created to determine whether consumer sensitive information was potentially compromised), Equifax mistakenly directed its Twitter followers to http://www.securityequifax2017.com/, a faux version of Equifax's website.

153. On September 15, 2017, Equifax announced the retirements of its Chief Information Officer and Chief Security Officer in connection with the Data Breach and its aftermath.[110] Soon after, on September 26, 2017, Equifax announced the retirement of its CEO, Richard Smith, less than three weeks after Equifax disclosed the Data Breach to the public.[111]

---

109 Janet Burns, *Equifax Was Linking Potential Breach Victims On Twitter To A Scam Site*, FORBES.COM (Sept. 21, 2017), https://www.forbes.com/sites/janetwburns/2017/09/21/equifax-was-linking-potential-breach-victims-on-twitter-to-a-scam-site/#bb68b87288f2.

110 *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, *supra* n.81.

111 Hamza Shaban, *Equifax CEO Richard Smith Steps Down Amid Hacking Scandal*, WASHINGTON POST (Sept. 26, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/09/26/equifax-ceo-retires-following-massive-data-breach/.

Post-Breach Investigations Reveal Equifax's Data Security Deficiencies

154. As a result of its investigation, Equifax identified deficiencies in its patch management policies and protocols that required immediate updates. To resolve its deficiencies, Equifax stated: "Vulnerability scanning and patch management processes and procedures have been enhanced, including an improvement to Equifax's patching procedures to require a 'closed loop' confirmation, which is applied to necessary patches."[112] In addition, the investigation revealed that Equifax entirely lacked adequate monitoring systems and controls necessary to detect the unauthorized infiltration and subsequent exfiltration of consumer data.

155. Senator Elizabeth Warren launched an investigation into the Equifax Data Breach and issued a report in February 2018, entitled *Bad Credit: Uncovering Equifax's Failure to Protect American's Personal Information* (the "Warren Report").[113] Senator Warren's investigation specifically found that Equifax "failed to take adequate steps to prevent the Data Breach" and that Equifax's information and security systems' suffered from numerous material deficiencies.

---

112 Equifax's Oct. 11, 2017 Responses, at 5, *supra* n.92.

113 Warren Report, *supra* n.58.

156. The Warren Report determined that Equifax adopted weak cybersecurity measures that failed to protect consumer data, and that such shortcomings were "a symptom of what appeared to be the low priority afforded cybersecurity by company leaders."[114]

157. The Warren Report noted that 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 past three years.[115] While Equifax's data security measures went underfunded, its shareholders profited handsomely. Equifax ultimately paid nearly twice as much in dividends to shareholders over the past three years than it spent on data security.[116]

158. The Warren Report, through consultation with cybersecurity experts, identified six weaknesses in Equifax's cybersecurity:

a. ***Faulty Patch Management Procedures*** – "For many vulnerabilities that arise in its software and applications, Equifax only has to deploy a software 'patch' that will fix the vulnerability and restrict access to the susceptible system . . . Yet Equifax let numerous software vulnerabilities sit un-patched for months at a time, leaving weakness through which hackers could gain access."

b. ***Feeble Monitoring of Endpoint and Email Security*** – Endpoint security refers to protecting a corporate network when it is accessed via

114 *Id.*

115 *Id.*

116 *Id.*

remote devices like laptops and mobile devices, as such devices can create a potential entry point for security threats. "Equifax failed to adopt strict endpoint and email security measure" to secure each endpoint on the network created by these devices.

c. ***Exposure of Sensitive Information*** – Equifax stored and "retained sensitive consumer information on easily accessible system" rather than segregating the most sensitive information into locations designed to limit access and maximize security.

d. ***Weak Network Segmentation*** – Equifax "failed to put security measures in place that would prevent hackers from jumping from insecure, internet-facing systems to backend databases that contain more valuable data. . . . Equifax's network segmentation measures failed to keep hackers from accessing consumer information because the company did not adopt adequately strict measures to protect valuable data."

e. ***Inadequate Credentialing*** – "Equifax's cybersecurity failures extended to their internal security. Each user on Equifax's system receives a set of privileges. Under strict security standards, Equifax would limit access to the most critical databases to just a handful of necessary users. This would protect the company from internal attacks and further bolster the company's overall data security regime. After gaining access to Equifax's systems, hackers then acquired user credentials – a username and password – and accessed a huge quantity of sensitive information using just those credentials. The company did not adopt adequately strict security measures to properly restrict user access to sensitive data."

f. ***Inadequate Logging*** – "Equifax neglected the use of robust logging techniques that could have allowed the company to expel the hackers from their systems and limited the size and scope of the data breach. Logging is a simple but crucial cybersecurity technique in which companies monitor their systems, continuously logging network access in order to identify unauthorized users. . . . 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."[117]

---

117 *Id.* at 3–4.

159. These findings by the Warren Report demonstrate that Equifax failed to comply with industry standards of care, as well as federal and state laws requiring the protection of consumer data.

160. Equifax's failures to adopt these industry-standard measures were more than mere mistakes; they were calculated decisions by Equifax executives to skirt data security in favor of paying out annual dividends. As noted in the Warren Report, "Equifax's goal, as stated by its CEO just weeks before he disclosed the Data Breach, was to go from '$4 billion in revenue to $8 billion' in approximately 5 years. Equifax prioritized growth and profits—but did not appear to prioritize cybersecurity."[118]

161. Former Equifax employees who worked on or alongside the Equifax security team agreed that Equifax did not place a high priority on data security. When asked about Equifax's data security risk tolerance, a former employee, who worked in IT at Equifax and is now a cybersecurity engineer, stated: "The degree of risk [Equifax] assumes is found, by most of the IT staff who worked elsewhere, to be preposterous."[119] Another former employee recounted how a 2016 Deloitte

---

118 *Id.*

119 Lorenzo Franceschi-Bicchierai, *Equifax Was Warned*, *supra* n.69; *see also* Cox, *Equifax Suffers Another Security Breach*, *supra* n.73.

security audit found several problems including a careless approach to patching systems. According to the employee: "Nobody took that security audit serious[ly] . . . . Every time there was a discussion about doing something, we had a tough time to get management to understand what we were even asking."[120] Another former Equifax employee commented: "It's a strange company. Given the amount of data they have access to and the sensitivity to us, security isn't at the forefront of everybody's mind, not how it should be."[121]

162. Equifax's Data Breach spawned several additional investigations. For example, federal regulators investigated Equifax's delayed notification about the Data Breach; the FBI is investigating the cause and extent of the Data Breach; and, Congress has held numerous hearings on the Equifax Data Breach.[122]

163. Numerous state attorneys general rebuked Equifax in the wake of the Data Breach. On September 18, 2017, New York Governor Andrew Cuomo directed the state's Department of Financial Services to develop a rule forcing credit reporting agencies to register with the state and comply with its cybersecurity

---

120 *Id.*

121 *Id.*

122 Andriotis & McMillan, *Hackers Entered Equifax Systems in March*, *supra* n.96.

requirements.[123] On September 19, 2017, attorneys general from 43 states and the District of Columbia signed a letter to Equifax, criticizing it for the Data Breach and its response.[124] The same day, Massachusetts Attorney General Maura Healey filed a suit against Equifax, seeking financial penalties and disgorgement of profits, alleging that Equifax failed to promptly notify the public of the Data Breach, failed to protect the personal data in its possession, and engaged in unfair and deceptive trade practices.[125]

164. Equifax's Data Breach is likely to be one of the most damaging data breaches in history, measured by both the sheer number of people exposed and the sensitivity and composition of the PII compromised: "[t]he Equifax hack is potentially the most dangerous of all, though, because the attackers were able to gain

---

123 Ashley Southall, *Cuomo Proposes Stricter Regulations for Credit Reporting Agencies*, NEW YORK TIMES (Sept. 18, 2017), https://www.nytimes.com/2017/09/18/nyregion/equifax-hack-credit-reporting-agencies-regulations.html.

124 Jack Suntrup, *Hawley, Madigan Criticize Equifax in Letter Signed by Other State Attorneys General*, ST. LOUIS POST-DISPATCH (Sept. 19, 2017), http://www.stltoday.com/business/national-and-international/hawley-madigan-criticize-equifax-in-letter-signed-by-other-state/article_868a0dbf-1ec6-57e0-87a7-6d008005f8f0.html.

125 David Lynch, *Equifax Faces Legal Onslaught from US States*, FINANCIAL TIMES (Sept. 21, 2017), https://www.ft.com/content/bf04768c-9e1b-11e7-8cd4-932067fbf946.

vast quantities of PII – names, addresses, Social Security numbers and dates of birth – at one time."[126]

165. Ultimately, the Equifax Data Breach was the result of a top-down policy to prioritize growth and profits over data security. As Equifax's CEO admitted, Equifax did not reduce the scope of sensitive data retained in backend databases.[127] The technical deficiencies and weaknesses that permitted unfettered access to Equifax's systems demonstrate the low priority Equifax gave to even rudimentary data security protocols, despite Equifax's role as one of the largest custodians of consumer data in the world.

166. Equifax did not employ reasonable measures that are critical to data security, including: vulnerability scanning and patch management processes and procedures; restrictions and controls for accessing critical databases; network segmentation between internet facing systems and backend databases and data stores; firewalls; file integrity monitoring; network, application, database, and

---

126 AnnaMaria Andriotis, Robert McMillan, & Christina Rexrode, *Equifax Hack Leaves Consumers, Financial Firms Scrambling*, THE WALL STREET JOURNAL (Sept. 8, 2017), https://www.wsj.com/articles/equifax-hack-leaves-consumers-financial-firms-scrambling-1504906993.

127 Equifax's Oct. 11, 2017 Responses, *supra* n.92.

system-level logging to monitor the network for unusual activity; and endpoint detection software to prevent exfiltration of data.[128]

167. But even the existence of these major security deficiencies does not explain how hackers were able to move around Equifax's servers unnoticed for more than 75 days while exfiltrating hundreds of millions of consumer records. Indeed, any routine and competent monitoring would have revealed to Equifax that there was significant irregular activity taking place on its servers.

168. Only now, after the damage has been done, has Equifax devoted the resources it originally should have earmarked to safeguard PII. In fact, as of March 31, 2018, Equifax recorded $113.3 million of pretax expenses related to the Data Breach.[129]

Equifax Failed to Comply with Industry Standards of Care as to Data Security

169. Equifax fully understood its duties to protect the confidentiality, accuracy, and integrity of PII. It serves as a linchpin of the U.S. economy, enabling financial institutions, like FI Plaintiffs and the Class, to extend credit and other financial services to U.S. consumers. It heralds itself as a "trusted steward" that is

128 *Smith Testimony*, *supra* n.1.

129 Equifax Inc., Quarterly Report (Form 10-Q) (April 26, 2018) at 19.

compliant with the laws requiring Equifax to adequately safeguard consumer data. In fact, however, Equifax violated federal and state data security requirements and disregarded reasonable data security standards of care.

170. One such reasonable data security standard of care is the NIST Guide to Enterprise Patch Management Technologies.[130] NIST develops standards and guidelines for the cost-effective security and privacy of information (other than national security-related information) for the federal government. The NIST Guide to Enterprise Patch Management Technologies advises organizations to timely implement patches because they "correct security and functionality problems in software and firmware. From a security perspective, patches are most often of interest because they are mitigating software flaw vulnerabilities; applying patches to eliminate these vulnerabilities significantly reduces the opportunities for exploitation."[131] Moreover, the NIST Guide to Enterprise Patch Management Technologies advises that "[o]rganizations should use other methods of confirming

130 Murugiah Souppaya and Karen Scarfone, *Guide to Enterprise Patch Management Technologies*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (July 2013), http://dx.doi.org/10.6028/NIST.SP.800-40r3.

131 *Id.*

[patch] installation, such as a vulnerability scanner that is independent from the patch management system."[132]

171. The NIST also has published a Guide to Application Whitelisting for computer security, which states that "application whitelisting software prevents installation and/or execution of any application that is not specifically authorized for use on a particular host. This mitigates multiple categories of threats, including malware and other unauthorized software."[133] NIST further recommends that "[o]rganizations should consider [application whitelisting] technologies, particularly for centrally managed desktops, laptops, and servers, because of the relative ease in managing these solutions and the minimal additional cost."[134]

172. The International Standards Organization ("ISO") and the International Electrotechnical Commission ("IEC") likewise have developed standards relating to information security management systems. ISO/IEC 27001 provides a checklist and comprehensive control objectives for information security policies that guide

---

132 *Id.*

133 Adam Sedgewick, Murugiah Souppaya, and Karen Scarfone, *Guide to Application Whitelisting*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Oct. 2015), http://dx.doi.org/10.6028/NIST.SP.800-167.

134 *Id.* at 5.

organizations in protecting their information systems and networks.[135] Specifically, the control objectives include:

> **A.5.1 Information Security Policy:** Objective: to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
>
> **A.6.1.1 Management Commitment to Information Security:** Control – Management shall actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.
>
> **A.10.3 System planning and acceptance:** Objective: To minimize the risk of systems failures.
>
> **A.10.3.2 System acceptance:** Control – Acceptance criteria for new information systems, upgrades, and new versions shall be established and suitable tests of the system(s) carried out during development and prior to acceptance.
>
> **A.10.4 Protection against malicious and mobile code:** Objective: To protect the integrity of software and information.
>
> **A.10.4.1 Controls against malicious code:** Control – Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented.
>
> **A.10.6 Network security management:** Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.

---

[135] ISO/IEC 27001 (2005), http://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/adeaf3e5_cc55_4222_8767_f26bcaec3f70/ISO_IEC_27001.pdf.

A.10.6.1 Network controls: Control – Networks shall be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

A.10.10 Monitoring: Objective: To detect unauthorized information processing activities.

A.10.10.1 Audit logging: Control – Audit logs recording user activities, exceptions, and information security events shall be produced and kept for an agreed period to assist in future investigations and access control monitoring.

A.11.4 Network access control: Objective: To prevent unauthorized access to networked services.

A.11.4.1 Policy on use of network services: Control – Users shall only be provided with access to the services that they have been specifically authorized to use.

A.11.4.7 Network routing control: Control – Routing controls shall be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

A.12.4 Security of system files: Objective: To ensure the security of system files.

A.12.4.1 Control of operational software: Control – There shall be procedures in place to control the installation of software on operational systems.

A.13.1 Reporting information security events and weaknesses: Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

> **A.13.1.1 Reporting information security events:** Control – Information security events shall be reported through appropriate management channels as quickly as possible.[136]

173. Similarly, ISO/IEC 27002 provides additional, specific best practice recommendations on information security management systems.[137] For example, ISO/IEC 27002 states that in order to properly protect against malicious and mobile code and to protect the integrity of software and the organization's information, the following guidance should be observed:

> Implementation guidance: Protection against malicious code should be based on malicious code detection and repair software, security awareness, and appropriate system access and change management controls.

174. Additionally, the Payment Card Industry Security Standards Council promulgates minimum standards. The Payment Card Industry Data Security Standards ("PCI DSS") apply to all organizations that store, process, or transmit Payment Card Data and provide minimum baseline standards of care to protect Payment Card Data.

175. PCI DSS 3.2, the version of the standards in effect beginning in April 2016, imposes the following 12 "high-level" mandates:

---

136 *Id.* at 13-26.

137 ISO/IEC 27002 (2005), http://www.slinfo.una.ac.cr/documentos/EIF402/ISO27001.pdf.

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

176. Furthermore, PCI DSS 3.2 sets forth detailed and comprehensive requirements that must be followed to meet each of the 12 mandates.

177. Among other things, PCI DSS required Equifax to properly secure Payment Card Data; not store cardholder data beyond the time necessary to authorize a transaction; implement proper network segmentation; encrypt Payment Card Information at the point-of-sale; restrict access to Payment Card Information to those with a need to know; and establish a process to identify and timely fix security vulnerabilities.

178. Equifax is a member of the PCI-DSS Security Council and, as such, clearly understood the requirements to protect PII and Payment Card Data.[138]

---

138 *Participating Organizations*, PCI SECURITY STANDARDS COUNCIL, https://www.pcisecuritystandards.org/get_involved/participating_organizations (last accessed May 30, 2018).

179. As discussed herein, Equifax failed to comply with the foregoing industry standards.

FI Plaintiffs Have Been, and Will Continue to Be, Harmed by the Equifax Data Breach

180. FI Plaintiffs and the Class provide consumers with a wide range of financial services, including deposit accounts, loans, and credit or debit cards. FI Plaintiffs and the Class are direct victims of Equifax's compromise of FI Plaintiff's customer data. As set forth above, in light of the fraudulent banking activity that FI Plaintiffs and the Class already have experienced and out-of-pocket costs that FI Plaintiffs and the Class already have suffered, there exists a certainly impending risk of future harm, in the form of future fraudulent banking activity, as a direct result of the Equifax Data Breach. Many of the actions FI Plaintiffs undertook after the Data Breach were the same precautions that various financial institution organizations, regulators, and experts recommended.

181. For example, experts recognized that identity authentication measures were jeopardized as a result of the Data Breach. According to Oliver Wyman, a management consulting firm, the Equifax Data Breach has profound implications for companies like FI Plaintiffs and the Class, "who use information stored by credit bureaus as a mechanism for confirming the identity of new and returning

customers."[139] It states that "there is a real question as to which commonly used identity-confirmation processes are still viable."[140] Even standard procedures for confirming identity that require customers to answer challenge questions based on the content of their credit files "are now far less safe as the underlying information has been hacked."[141]

182. The Credit Union Executive Society ("CUES") concludes that credit unions and other financial institutions will be subject to increased fraud and well-disguised fraud attempts as a result of the Equifax Data Breach.[142] Specifically, CUES states that because "the stolen information is personal credit bureau data that lasts a consumers' entire lifetime . . . the foundation that banks and credit unions use to control new account fraud or application fraud is badly damaged."[143]

---

139 Paul Mee & Chris DeBrusk, *The Equifax Data Breach And Its Impact On Identity Verification*, OLIVER WYMAN (Sept. 2017), https://www.marsh.com/content/dam/oliver-wyman/v2/publications/2017/sep/Oliver_Wyman_Equifax_Data_Breach.pdf.

140 *Id*.

141 *Id*.

142 Frank McKenna, *Planning, Post Equifax*, 40 CREDIT UNION MGMT. MAGAZINE (Oct. 2017), https://www.cues.org/article/viewalldd/planning-post-equifax.

143 *Id*.

183. One commentator explained: "Banks are going to pay the most of anyone."[144] This is because it is ultimately financial institutions, and not the consumers, that bear the risk of loss if identity thieves open accounts, transfer funds, take out loans, or obtain credit or debit cards.[145]

184. A report by the Department of Justice found that fraudulent use of existing account information, including credit card and bank account information, affected 86% of identity theft victims in 2014.[146]

185. Another commentator confirmed that as a direct result of the Data Breach, financial institutions face an increased risk of new account fraud and the fraudulent transactions that inevitably result:

> After the 2017 Equifax hacking scandal, experts say consumers increasingly need to be on the lookout for phantom bank accounts, mysterious credit cards and other gruesome things. And remember, scammers don't walk around in gory masks with fake blood dripping off their teeth. . . . A phantom account is when someone, not you, opens a bank account in your name using your ID. Ken Tumin, founder and

---

144 Joe Ruben, *BankThink Fallout from Equifax Breach Will Hit Banks Hardest*, AMERICAN BANKER (Sept. 29, 2017), https://www.americanbanker.com/opinion/fallout-from-equifax-breach-will-hit-banks-hardest.

145 *See, e.g.*, *id.*

146 Erika Harrell, *Victims of Identity Theft, 2014*, U.S. DEPARTMENT OF JUSTICE, BUREAU OF JUSTICE STATISTICS, NCJ 248991 at 1 (Sept. 2015), https://www.bjs.gov/content/pub/pdf/vit14.pdf.

> editor of DepositAccounts.com, said sometimes a criminal will open a checking account using your ID and then possibly attempt to link to another one of your accounts to try to withdraw money.[147]

186. Indeed, financial institutions are in a unique position because they are the ones who reimbursed consumers whose PII or Payment Card Data was compromised in the Data Breach for fraud losses that are incurred in connection with accounts held at their financial institutions, as discussed herein. *See*, *e.g.*, 15 U.S.C. §§1643 & 1693g.

187. Further, FI Plaintiffs and the Class are subject to the same regulatory requirements that Equifax is subject to, as set forth in paragraphs 56 through 66, above.

188. Equifax knew that FI Plaintiffs, as payment card issuers, lenders, and deposit account holders, would bear the ultimate responsibility for identity theft and fraudulent lending and other fraudulent consumer transactions if Equifax failed to protect their customers' PII and Payment Card Data.

189. Equifax acknowledges that this type of harm is a reality for financial institutions when PII is compromised:

---

147 Susan Tompor, *Something Evil Lurks in Fake Checks and Phantom Financial Doings*, DETROIT FREE PRESS (Oct. 26, 2017), https://www.freep.com/story/money/personal-finance/susan-tompor/2017/10/26/fake-checks-phantom-bank-accounts-other-tricks/789905001/.

> Fraudsters can build synthetic identities by creating a fake SSN or obtaining/stealing a real SSN and adding non-matching identifying information such as name, date of birth, and address. Perpetrators often prefer to steal randomized SSNs or purchase them from hackers who breach public or private databases that contain personally identifiable information. Then the fraudster uses the synthetic identity to apply for a line of credit, typically at a bank. The bank submits an inquiry to credit bureaus about the applicant's credit history. The credit bureaus initially report that an associated profile does not exist and the bank may reject the application; however, the credit inquiry generates a credit profile for the synthetic identity in the credit bureaus' databases. At this stage, the perpetrator will typically apply for multiple credit cards and other products marketed to consumers who are new to credit. They maintain good credit over time to build up credit limits and apply for more cards. Most times, the fraudster ends up charging the maximum amount on credit cards and not paying the bill (known as "bust-out" fraud) or they may launder the money between multiple accounts.[148]

190. In a 2015 publication, Equifax explained to financial institutions:

> Data breaches which expose personally identifiable information (PII) are a growing problem in today's high tech world. . . . ***The PII captured from data breaches is often used for both identity theft and synthetic identity creation to open or access financial accounts***. ***Once a fraudster steals or creates an identity and is inside a financial system, they can wreck endless damage***. A key point at which financial institutions must combat identity theft and synthetic identity creation fraud is during the vulnerable point when customers open new accounts."[149] [Emphasis added].

---

148 Donahoo, *How Fraudsters Are Using Synthetic Identities*, *supra* n.2.

149 Sally Ewalt, *Data Breaches Increase Fraud Threats*, INSIGHTS BLOG (Dec. 1, 2015), https://insight.equifax.com/data-breaches-increase-fraud-threats/.

191. Given the scale of the PII compromised in the Equifax Data Breach was unprecedented and the fact that FI Plaintiffs and the Class already have experienced fraudulent banking activity, FI Plaintiffs and the Class had to take immediate action and incur costs to mitigate and avoid the substantial risk of future harm caused by the Data Breach.

192. In the wake of the Data Breach, experts and regulators provided guidance to financial institutions of suggested mitigation efforts.

193. For instance, one publication explained that the Equifax Data Breach has had a particularly significant impact on the measures financial institutions use to authenticate new and potential customers. Security experts warned that "the scale of the Equifax breach means that every SSN in the United States – together with the accompanying name – must be presumed to be public knowledge, and thus should not be used to validate anyone's identity, ever again."[150]

194. CUES advised that fraud managers at financial institutions should plan for and adopt heightened fraud detection methods because, as a direct result of the

[150] Mathew J. Schwartz, *Equifax Breach: 8 Takeaways*, BANK INFO SECURITY (Sept. 8, 2017), https://www.bankinfosecurity.com/equifax-breach-8-takeaways-a-10278; *see also* Mee & DeBrusk, *The Equifax Data Breach And Its Impact On Identity Verification*, *supra* n.139.

Data Breach: (1) knowledge-based authentication tools will be less effective; (2) increased new account and new loan application fraud will occur; and (3) credit card fraud will increase.[151]

195. The American Bankers Association ("ABA") recommended that banks should: (1) assess and analyze the impact of the Data Breach in order to "detect potential risks to the bank and its customers"; (2) enhance account monitoring activities "with a particular emphasis on preventing new account identity theft, synthetic identity theft, and takeover of bank and credit accounts"; (3) anticipate credit report freezes, which "may slow the review of credit applications and create compliance timing complications, particularly for mortgage loans"; and (4) update their identity theft red flag program.[152]

196. The ABA also met with representatives from federal banking agencies and published an article detailing what regulators expected from banks as a result of the Equifax Data Breach, including:

---

151 McKenna, *supra* n.142.

152 Krista Shonk & Nessa Feddis, *Third-Party Tactics: Tips for Managing the Equifax Breach*, ABA BANKING JOURNAL (Nov. 2, 2017), https://bankingjournal.aba.com/2017/11/third-party-tactics-tips-for-managing-the-equifax-breach/.

a. "Given the scope of the [Equifax] cyberattack, all banks will have a substantial percentage of customers whose information was breached. As a result, regulators are immediately focused on bank efforts to improve fraud detection and prevention;" and

b. "Banks should . . . enhance their antifraud activities, with a particular emphasis on preventing new account identity theft, and takeover of bank and credit accounts." [153]

197. The regulators further advised that, as a result of the Data Breach, "[c]onsumers may freeze their credit reports in an effort to protect against identity theft. These freezes may slow the review of credit applications and create compliance timing complications, particularly for mortgage loans."[154]

198. The New York State Department of Financial Services ("NYDFS") recognized the "seriousness of [the Equifax] breach" and the "potential harm to consumers and financial institutions." It issued guidance to urge "financial institutions to take immediate action and consider precautions to protect consumers

153 *Id.*

154 *Id.*

in light of the cybersecurity attack at Equifax that compromised the personal information of millions of Americans."[155]

199. NYDFS explained that "financial institutions can no longer just rely on personally identifiable information (PII) as a means of verifying a person's identity" and it encouraged financial institutions, if appropriate, to "consider using an identity verification/fraud service for identity verification."[156]

200. The American Banker explained that, as a result of the risk created by the Data Breach, banks will need to implement stricter authentication procedures.[157]

201. It further expounded:

> "Financial institutions and other similar businesses that rely on personally identifiable information are being confronted with an environment where all of this data is being bought and sold, fed by these types of events," said Al Pascual, senior vice president, research director and head of fraud and security at Javelin Strategy & Research.

---

155 New York State Department of Financial Services, *Press Release: DFS Urges Financial Institutions to Take Immediate Steps to Protect Sensitive Consumer Data in Light of Equifax Cyberattack* (September 18, 2017), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr1709182.

156 *Id.*

157 Ruben, *BankThink Fallout from Equifax Breach Will Hit Banks Hardest*, *supra* n.144.

> That means ***they can no longer rely strictly on PII any longer as a means of verifying identity***.[158] [Emphasis added].

202. After the Data Breach, experts also stated that FI Plaintiffs and the Class would suffer increased delays and decreased revenues from the increase in credit freezes by consumers impacted by the Data Breach, explaining that a credit freeze was one of the most commonly suggested ways for consumers to protect themselves, but the effect is that it often slows down credit applications and delays the loan process.[159]

203. Equifax itself has directed consumers to "[c]onsider placing a security freeze . . . on your credit report."[160]

204. Credit freezes can lead to reduced revenues for financial institutions as they are not able to efficiently complete credit applications:

> Consumers may freeze their credit reports in an effort to protect against identity theft. These freezes may slow the review of credit applications and create compliance timing complications, particularly for mortgage loans. As a result, banks should review their credit application processes and be

---

158 Penny Crossman, *Seven Aftershocks of the Equifax Breach*, American Banker (Sept. 8, 2017), https://www.americanbanker.com/news/seven-aftershocks-of-the-equifax-breach-what-bankers-need-to-know.

159 Ruben, *BankThink Fallout from Equifax Breach Will Hit Banks Hardest*, *supra* n.144.

160 *2017 Cybersecurity Incident & Important Consumer Information*, EQUIFAX INC., https://www.equifaxsecurity2017.com/ (last accessed May 30, 2018).

prepared to address questions and expectations of customers who have frozen their credit reports.[161]

205. The CRAs also acknowledge that credit freezes "may delay, interfere with or prohibit the timely approval" of a range of services, including "a new loan, credit, mortgage, insurance, government services or payments, rental housing, employment, investment, license, cellular telephone, utilities, digital signature, Internet credit card transaction or other services, including an extension of credit at point of sale."[162]

206. One study found that nearly 20% of Americans (almost 65 million people) froze their credit as a direct result of the Data Breach.[163]

207. That same study explained the "significant trouble" the credit freezing causes for the lending industry, like FI Plaintiffs and the Class, because it makes it difficult to assess risk and slows down the approval and loan process.[164]

---

161 Shonk & Feddis, *Third-Party Tactics*, *supra* n.152.

162 *Security Freeze*, EXPERIAN INFORMATION SOLUTIONS, INC., https://www.experian.com/blogs/ask-experian/credit-education/preventing-fraud/security-freeze/ (last accessed May 30, 2018).

163 Fundera, Inc., Resources, *Nearly 1 in 5 Americans Froze Credit After Data Breach* (March 6, 2018), https://www.fundera.com/resources/credit-freeze-after-equifax-breach?nocache

164 *Id.*

208. The repercussions from the Data Breach, which already has harmed FI Plaintiffs, will be long lasting.[165] According to Nick Clements, who formerly ran a fraud department at Citigroup:

> This stuff takes time[.] . . . If names and Social Security numbers and dates of birth are out there, they will be used at some point. No one should take reassurance that a few weeks in, they don't detect a high level of activity. . . . There's a long shelf life here.[166]

209. Commentators have stated that the Equifax Data Breach will result in long term added costs to the credit authentication and verification activities conducted by financial institutions:

> [I]n most cases lenders will likely interpret "better authentication" as requiring more data from consumers to help ensure that the applicant is indeed who he says he is. For example, lenders may ask consumers to respond to more out-of-wallet questions during the application process that are more difficult for an identity thief to answer, like, "What is your mortgage payment?" or "Did you own a certain type of car? This process will require consumers to provide more information to prove their identity. More disclosure of information from consumers will slow down the lending process because consumers may need to gather more information to complete the process and because it will also take them more time to fill in lender requirements. Requiring consumers to disclose more information could lead consumers to abandon credit applications that are otherwise supposed to be quick and painless, such

---

165 Crosman, *Seven Aftershocks of the Equifax Breach: What bankers need to know*, *supra* n.158, https://www.americanbanker.com/news/seven-aftershocks-of-the-equifax-breach-what-bankers-need-to-know; Ruben, *BankThink Fallout from Equifax Breach Will Hit Banks Hardest*, *supra* n.144.

166 Crossman, *Seven Aftershocks of the Equifax Breach*, *supra* n.158.

> as the process for obtaining instant retail credit. Specifically, a less convenient process in addition to heightened consumer fears about their data being hacked could discourage consumers from completing a loan application unless it is a credit line they absolutely must have. [167]

210. FI Plaintiffs and the Class already have experienced fraudulent banking activity and incurred direct out-of-pocket costs to reimburse customers for fraudulent transactions and to mitigate the substantial and certainly impending risk of additional harm created by the Data Breach, in the form of future fraudulent banking activity.

211. FI Plaintiffs and the Class have been injured, suffering financial losses directly attributable to the Data Breach. Specifically, because their customers' PII and/or Payment Card Data was compromised in the Data Breach and consistent with the guidance provided by experts and regulators, FI Plaintiffs have incurred direct out-of-pocket costs associated with: cancelling and reissuing payment cards; reimbursing customers whose payment cards were compromised in the Data Breach for fraudulent transactions; reimbursing customers whose PII was stolen in the Data Breach for fraudulent transactions; lost revenues due to abandoned or delayed credit applications from customers who froze their credit reports in the wake of the Data Breach and were subsequently unable to unfreeze their credit reports in a timely

---

[167] Ruben, *BankThink Fallout from Equifax Breach Will Hit Banks Hardest*, *supra* n.144.

fashion; increased staffing to respond to theft of customers' PII in the wake of the Data Breach; enhancing their customer verification procedures and retraining staff regarding these procedures; purchasing identity authentication, identity theft protection, or fraud detection and prevention software tools; and/or purchasing cyber security insurance.

212. FI Plaintiffs ASI Federal Credit Union, Consumers Cooperative Credit Union, DL Evans Bank, Financial Health Federal Credit Union, First Financial Credit Union, The First State Bank, Peach State Federal Credit Union, Texas First Bank, The Summit Federal Credit Union, and TruEnergy Federal Credit Union and members of the Class have incurred direct out-of-pocket costs to purchase new or enhanced identity authentication, identity theft protection, or fraud detection and prevention services and/or revised their methods of identity authentication or fraud prevention.

213. FI Plaintiffs First Financial Credit Union, Hudson River Community Credit Union, and The Summit Federal Credit Union and members of the Class have incurred direct out-of-pocket costs to reimburse their customers whose PII was compromised in the Data Breach for fraudulent transactions.

214. FI Plaintiffs ASI Federal Credit Union, Consumers Cooperative, Hudson River Community Credit Union, Peach State Federal Credit Union, The

Summit Federal Credit Union, Texas First Bank, and TruEnergy Federal Credit Union have incurred direct out-of-pocket costs to cancel and reissue payment cards that were compromised in the Data Breach, and Class members that issued payment cards that were impacted in the Data Breach also have incurred direct out-of-pocket costs to: cancel and create new payment cards (and new uniquely-identifiable data); close or otherwise protect any deposit, transaction, checking, or other affected payment card accounts; refund any cardholder for any fraudulent transactions; respond to a higher volume of cardholder complaints, confusion, and concern; and increase fraud monitoring efforts with regard to the compromised payment cards.

215. FI Plaintiffs and the Class have suffered, and will continue to suffer, lost profits and reputational harm as a result of the Data Breach. Specifically, FI Plaintiffs DL Evans Bank, Financial Health Federal Credit Union, The First State Bank, Peach State Federal Credit Union, and TruEnergy Federal Credit Union lost revenues due to abandoned or delayed credit applications from customers who froze their credit reports in the wake of the Data Breach and were subsequently unable to unfreeze their credit reports in a timely fashion. In the wake of the Data Breach, Equifax and others have directed consumers to "[c]onsider placing a security

freeze . . . on your credit report."[168] As CRAs acknowledge, however, credit freezes "may delay, interfere with or prohibit the timely approval" of a range of services, including "a new loan, credit, mortgage, insurance, government services or payments, rental housing, employment, investment, license, cellular telephone, utilities, digital signature, Internet credit card transaction or other services, including an extension of credit at point of sale."[169]

216. In sum, the Equifax Data Breach has damaged FI Plaintiffs and created a certainly impending risk of future harm in the form of fraudulent banking activity, which has occurred and will continue to occur, in the immediate and foreseeable future, to FI Plaintiffs and the Class. FI Plaintiffs and the Class therefore seek damages and injunctive relief for Equifax's negligence, negligence per se, negligent misrepresentation, and violation of state unfair and deceptive trade practices statutes. The Association Plaintiffs join FI Plaintiffs and the Class in seeking a declaratory judgment and equitable relief.

---

168 *2017 Cybersecurity Incident & Important Consumer Information*, EQUIFAX INC., https://www.equifaxsecurity2017.com/ (last accessed May 30, 2018).

169 *Security Freeze*, *supra* n.162.

CLASS ACTION ALLEGATIONS

217. FI Plaintiffs bring this action on behalf of themselves and as a class action under Federal Rules of Civil Procedure 23(a), (b)(2), and (b)(3), on behalf of the following nationwide class ("Nationwide Class" or the "Class"):

FI Plaintiffs Nationwide Class

> All Financial Institutions in the United States (including its Territories and the District of Columbia) whose customers' PII and/or Payment Card Data was exposed as a result of the Equifax Data Breach announced on or about September 7, 2017.

The Nationwide Class asserts claims against Equifax for negligence (Count 1), negligence per se (Count 2), and negligent misrepresentation (Count 3). The Nationwide Class also requests a declaratory judgment (Count 9) and reasonable attorneys' fees and the expenses of litigation (Count 10).

218. The Plaintiffs identified in Counts 4-8 also bring this action on behalf of themselves and as a class action under Federal Rules of Civil Procedure 23(a), (b)(2), and (b)(3), on behalf of statewide classes ("Statewide Subclasses" or "Subclasses") (collectively with the Nationwide Class, the "Classes") for violation of the unfair and deceptive business practices statutes in Georgia, Illinois, Louisiana, New Mexico, and New York, defined as follows:

FI Plaintiffs Statewide Subclasses

> All Financial Institutions in [name of state] whose customers' PII and/or Payment Card Data was exposed as a result of the Equifax Data Breach announced on or about September 7, 2017.

219. Excluded from the Nationwide Class and each Subclass are Equifax, any entity in which Equifax has a controlling interest, and Equifax's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Nationwide Class and each Subclass are any judicial officer presiding over this matter, members of their immediate family, and members of their judicial staff.

Rule 23(a)

220. This action may properly be maintained as a class action and satisfies the requirements of Fed. R. Civ. P. 23(a): numerosity, commonality, typicality, and adequacy.

221. **Numerosity.** The members of the Class and each Subclass are so numerous and geographically dispersed that joinder would be impracticable. The number of Class members exceeds 10,000 and each Subclass has at least fifty members.

222. **Commonality and Predominance.** There are common questions of law and fact that predominate over questions affecting only individual Class and

Subclass members. These common legal and factual questions include, but are not limited to:

a. whether Equifax owed a duty to use reasonable care to avoid causing foreseeable risk of harm to FI Plaintiffs and members of the Class when obtaining, storing, using, and managing PII and Payment Card Data, including taking action to safeguard such data;

b. whether Equifax actively mishandled PII and implemented and maintained data security measures that it knew or should have known were unreasonable and inadequate to protect PII and Payment Card Data;

c. whether Equifax negligently allowed PII and Payment Card Data to be accessed, used, or disclosed by third parties;

d. whether FI Plaintiffs and members of the Class justifiably relied on representations made by Equifax as to its data security practices and the integrity and accuracy of information Equifax provided;

e. whether Equifax intended that FI Plaintiffs and members of the Class would rely on Equifax's representations as to its data

security practices and the integrity and accuracy of information Equifax provided;

f. whether Equifax failed to adequately notify FI Plaintiffs and members of the Class and Subclasses that its data systems were breached;

g. whether FI Plaintiffs and members of the Class and Subclasses were injured and suffered damages and ascertainable losses;

h. whether Equifax's actions and inactions failed to provide reasonable security proximately caused the injuries suffered by FI Plaintiffs and members of the Class and Subclasses;

i. whether FI Plaintiffs and members of the Class and Subclasses are entitled to damages and, if so, the measure of such damages; and

j. whether FI Plaintiffs and members of the Class and Subclasses are entitled to injunctive, equitable, declaratory and/or other relief, and if so, the nature of such relief.

223. **Typicality.** FI Plaintiffs' claims are typical of the claims of the absent class members and have a common origin and basis. FI Plaintiffs and absent Class and Subclass members are all financial institutions injured by Equifax's Data

Breach. The FI Plaintiffs' claims arise from the same practices and course of conduct giving rise to the claims of the absent Class and Subclass members and are based on the same legal theories, namely the Equifax Data Breach. If prosecuted individually, the claims of each Class and Subclass member would necessarily rely upon the same material facts and legal theories and seek the same relief. FI Plaintiffs' claims arise from the same practices and course of conduct that give rise to the other Class and Subclass members' claims and are based on the same legal theories.

224. **Adequacy.** FI Plaintiffs will fully and adequately assert and protect the interests of the absent Class and Subclass members and have retained Class counsel who are experienced and qualified in prosecuting class action cases similar to this one. Neither FI Plaintiffs nor their attorneys have any interests contrary to or conflicting with the interests of absent Class or Subclass members.

Rule 23(b)(3)

225. The questions of law and fact common to all Class and Subclass members predominate over any questions affecting only individual class members.

226. A class action is superior to all other available methods for the fair and efficient adjudication of this lawsuit because individual litigation of the absent Class and Subclass members' claims is economically infeasible and procedurally

impracticable. Class and Subclass members share the same factual and legal issues and litigating the claims together will prevent varying, inconsistent, or contradictory judgments, and will prevent delay and expense to all parties and the court system through litigating multiple trials on the same legal and factual issues. Class treatment will also permit Class and Subclass members to litigate their claims where it would otherwise be too expensive or inefficient to do so. FI Plaintiffs know of no difficulties in managing this action that would preclude its maintenance as a class action.

Rule 23(b)(2)

227. All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for Equifax. Such individual actions would create a risk of adjudications that would be dispositive of the interests of other Class members and impair their interests. Defendants, through their uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

228. Contact information for each Class member, including mailing addresses, is readily available, facilitating notice of the pendency of this action.

CHOICE OF LAW FOR NATIONWIDE CLAIMS

229. The State of Georgia has a significant interest in regulating the conduct of businesses operating within its borders. Georgia, which seeks to protect the rights and interests of Georgia and all residents and citizens of the United States against a company headquartered and doing business in Georgia, has a greater interest in the nationwide claims of Plaintiffs and Nationwide Class members than any other state and is most intimately concerned with the claims and outcome of this litigation.

230. The principal place of business of Equifax, located at 1550 Peachtree Street NW, Atlanta, Georgia, is the "nerve center" of its business activities – the place where its high-level officers direct, control, and coordinate the corporation's activities, including its data security functions and major policy, financial, and legal decisions.

231. Equifax's data centers were located in Alpharetta, Georgia. MAJORITY STAFF OF U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM, 115th CONGRESS, THE EQUIFAX DATA BREACH, at 31 & n.166 (Comm. Print 2018). Equifax's response to the Data Breach at issue here, and corporate decisions surrounding such response, were made from and in Georgia.

232. Equifax's breaches of duty to Plaintiffs and Nationwide Class members emanated from Georgia.

233. Application of Georgia law to the Nationwide Class with respect to Plaintiffs' and Class members' claims is neither arbitrary nor fundamentally unfair because Georgia has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiffs and the Nationwide Class.

234. Under Georgia's choice of law principles, which are applicable to this action, the common law of Georgia applies to the nationwide common law claims of all Nationwide Class members. Additionally, given Georgia's significant interest in regulating the conduct of businesses operating within its borders, Georgia common law may be applied to non-resident consumer plaintiffs.

LEGAL CLAIMS

COUNT 1

Negligence

(On behalf of FI Plaintiffs and the FI Plaintiffs Nationwide Class)

235. FI Plaintiffs repeat and reallege each and every allegation contained above as if fully set forth herein.

236. Equifax owes a common law duty to use reasonable care to avoid causing foreseeable risk of harm to FI Plaintiffs and members of the Class when obtaining, storing, using, selling, and managing PII and Payment Card Data, including taking action to reasonably safeguard such data and providing notification

to FI Plaintiffs and the Class of any breach in a timely manner so that appropriate action can be taken to minimize or avoid losses. This duty arises from several sources (described below) and is independent of any duty Equifax owed as a result of any contractual obligations.

237. This duty extends to protecting others against the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where an actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, where the actor is in possession of something valuable that affords a peculiar temptation for criminal interference, or where the parties are in a special relationship. *See* Restatement (Second) of Torts §302B. Numerous courts and legislatures also have recognized the existence of a specific duty to reasonably safeguard PII, Payment Card Data, and other sensitive information.

238. Equifax's sole business purpose is to collect, store, use, maintain, sell, and transmit consumer PII. Equifax holds itself out as one of the three nationwide CRAs that serve as linchpins of the financial system. In this role, Equifax was entrusted with sensitive and valuable PII regarding hundreds of millions of consumers. FI Plaintiffs and the Class, who provide various financial services, including the extension of credit, to the same consumers whose PII was

compromised as a result of the Equifax Data Breach, are in a symbiotic relationship with Equifax. Equifax strongly encourages financial institutions to furnish Equifax with their consumer data so that Equifax can provide accurate and reliable information to financial institutions, which rely on the integrity of the credit reporting system to extend credit and provide other financial services.

239. Thus, the common law duty to use reasonable care to avoid causing foreseeable risk of harm exists in this case because FI Plaintiffs and members of the Class were the foreseeable and probable victims of any data breach of Equifax's systems that occurred as a result of Equifax's inadequate data security practices. In fact, Equifax knew it was more likely than not that FI Plaintiffs and members of the Class would be harmed by a breach of Equifax's systems given the highly valuable and sensitive data it collected. Indeed, Equifax calls itself a "trusted steward" of data and markets numerous fraud and identity theft prevention and protection solutions directly to financial institutions. Equifax also knew that it was in possession of one of the most valuable collections of data in the world, and that Equifax's systems would therefore be tempting targets for data thieves.

240. It was foreseeable that injury to FI Plaintiffs and the Class would result from Equifax's active mishandling of PII and Payment Card Data, including, but not limited to, not using reasonable security measures to protect such PII and Payment

Card Data and to provide timely notice of the Data Breach. Indeed, Equifax acknowledged the risk of a data breach and the impact such a breach could have on Equifax, consumers, and financial institutions, like FI Plaintiffs and the Class, in its 2016 Form 10-K filed with the SEC.

241. In the current environment where data breaches are near commonplace (as discussed above), Equifax knew or should have known of the significant risk that its computer systems would be breached, particularly in light of the numerous data breach incidents it experienced prior to the Data Breach.

242. Equifax's duty to act reasonably in managing consumer data and to use reasonable data security measures also arises under the GLBA, 15 U.S.C. §§6801-6809, and its implementing regulations, 16 C.F.R. Part 314 (the "Safeguards Rule"), which "sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information" and "applies to the handling of customer information by all financial institutions over which the [FTC] has jurisdiction." 16 C.F.R. §314.1(a)-(b). Equifax is a financial institution, as defined in Section 509(3)(A) of the GLBA, 15 U.S.C. §6809(3)(A).

243. The Safeguards Rule "applies to all customer information in [a financial institution's] possession, regardless of whether such information pertains to

individuals with whom [a financial institution has] a customer relationship, or pertains to the customers of other financial institutions that have provided such information to [the subject financial institution]." 16 C.F.R. §314.1(b).

244. The Safeguards Rule requires financial institutions to "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to [the financial institution's] size and complexity, the nature and scope of [the financial institution's] activities, and the sensitivity of any customer information at issue." 16 C.F.R. 314.3(a).

245. Specifically, the Safeguards Rule requires a financial institution, among other things, to:

> (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:
>
> > (1) Employee training and management;
> >
> > (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

> (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.
>
> (c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
>
> * * *
>
> (e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program. 16 C.F.R. 314.4.

246. As alleged herein, Equifax breached its duties under the GLBA and the Safeguards Rule. The security program and safeguards Equifax maintained were not appropriate to Equifax's size and complexity, the nature and scope of its business, and the sensitivity of the PII of the hundreds of millions of U.S. consumers that it obtains, stores, uses, transmits, sells, and manages. As alleged above, Equifax's security program and safeguards were not adequate to: identify reasonably foreseeable internal and external risks, assess the sufficiency of safeguards in place to control for these risks, or to detect, prevent, or respond to a data breach. In particular, Equifax's security program and safeguards were inadequate to evaluate and adjust to events that would have a material impact on Equifax's information

security program, such as the numerous prior data breaches that other retailers and Equifax itself had experienced and the notification to Equifax that an identified vulnerability in a software program it utilized would make Equifax particularly susceptible to a data breach.

247. Equifax's duty to act reasonably in handling consumer data and to use reasonable data security measures also arises under Section 5 of the FTC Act, 15 U.S.C. §45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of not acting reasonably in the management of the data, and not using reasonable security measures to protect such data, by companies such as Equifax.

248. FTC guidelines, publications, and consent orders further form the basis of Equifax's duty and a corresponding reasonable standard of care.

249. In 2007, the FTC published guidelines which establish reasonable data security practices for businesses. The guidelines, which were updated in October 2016, note businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vender-approved patches to correct security problems. The guidelines also recommend that businesses consider

using an intrusion detection system to identify a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[170]

250. The FTC also has published a document entitled "FTC Facts for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

251. And the FTC has issued orders against businesses that failed to employ reasonable measures to secure customer data. These orders provide further guidance to businesses with regard to their data security obligations.

252. In addition, individual states have enacted statutes based on the FTC Act and/or that otherwise require Equifax to act reasonably in the management of the data, and to use reasonable security measures to protect such data, as detailed herein, that also created a duty.

---

[170] FTC, Protecting Personal Information: A Guide for Business (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

253. Equifax's duty to act reasonably in handling consumer data and to use reasonable data security measures also arises under the FCRA, 18 U.S.C. §1681, which regulates the collection, dissemination, and use of credit information. The FCRA explicitly recognizes a duty by Equifax, which is subject to the FCRA as a CRA as defined in 15 U.S.C. §§1681a(f) and (p), to maintain reasonable procedures in order to protect the confidentiality, accuracy and proper use of credit information.

> (b) Reasonable procedures
>
> It is the purpose of this subchapter to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of this subchapter.

15 U.S.C. §1681.

254. As alleged in detail herein, Equifax's security practices and procedures were so severely deficient or nonexistent, despite its knowledge that this PII was coveted by attackers and certain to be subject to attempted hacks and exfiltration, that Equifax violated its duty to maintain reasonable procedures in order to protect the confidentiality, accuracy and proper use of credit information.

255. In fact, Equifax affirmatively assumed the duty to act with reasonable care in managing its data, and to use reasonable security measures to protect such

data, as expressed in its public statements where it acknowledges that it is bound by the GLBA. In its privacy policies Equifax repeatedly states it uses "reasonable physical, technical and procedural safeguards to help protect" PII, which language is identical to that in the GLBA's Safeguards Rule. Through these and other statements alleged herein, Equifax specifically assumed the duty to comply with the data security industry standards that are applicable to a company whose sole business is transacting in PII. FI Plaintiffs have alleged herein several industry standards of care with which Equifax has not complied.

256. In public statements, Equifax admits that it has an enormous responsibility to protect consumer PII, that it is entrusted with this data, and that it did not live up to its responsibility to protect PII.

257. A duty to act reasonably in the management of the data, and to use reasonable security measures to protect such data, also arises as a result of the special relationship that existed between Equifax and FI Plaintiffs and the Class. This special relationship exists because financial institutions entrust credit bureaus like Equifax with customer PII and Equifax is in a unique position as one of only three nationwide credit reporting companies that serve as the linchpins of the financial system. Because of its crucial role within the credit system, Equifax was in a unique and superior position to protect against the harm suffered by FI Plaintiffs and the

Class as a result of the Equifax Data Breach. Indeed, ***only*** Equifax was in a position to ensure that its systems were sufficient to protect its primary asset – consumer PII.

258. Equifax breached its common law and statutory duties and industry standards of care – and was negligent – by actively mishandling the consumer data and failing to use reasonable measures to protect consumers' personal and financial information from the hackers who perpetrated the Data Breach and by failing to provide timely notice of the Data Breach. Equifax mishandled its data management and IT systems by adopting and maintaining data security measures that Equifax knew or should have known were unreasonable and inadequate to protect PII and Payment Card Data. The specific affirmative negligent acts and omissions committed by Equifax include, but are not limited to, the following:

a. Intentionally ignoring warnings about specific vulnerabilities in its systems identified by Equifax's own employees, consultants, and software vendors;

b. Maintaining (i) faulty patch management procedures, (ii) an insufficient firewall, (iii) feeble monitoring of endpoints and non-existent exfiltration monitoring, (iv) weak network segmentation, (v) inadequate monitoring and logging of network

access, and (vi) insufficiently strict credentialing procedures that failed to restrict access to those with a valid purpose;

c. Refusing to timely and adequately update security certificates on key systems;

d. Storing and retaining PII in easily accessible systems rather than segregating it into locations with limited access and maximum security measures; and

e. Failing to disclose the Data Breach in a timely manner.

259. As a result of the foregoing acts, Equifax breached its common law and statutory duties to act reasonably in the management of the data, and to use reasonable security measures to protect such data.

260. As a direct and proximate result of Equifax's negligent acts of misfeasance and nonfeasance, FI Plaintiffs and the Class have suffered and continue to suffer injury and damages as described herein.

261. Because no statutes of other states are implicated, Georgia common law applies to the negligence claims of FI Plaintiffs and the Class.

COUNT 2

Negligence Per Se

(On behalf of FI Plaintiffs and the FI Plaintiffs Nationwide Class)

262. FI Plaintiffs repeat and reallege each and every allegation contained above as if fully set forth herein.

263. Equifax is a financial institution, as defined in Section 509(3)(A) of the GLBA, 15 U.S.C. §6809(3)(A).

264. Equifax has a duty to act reasonably in handling consumer data and to use reasonable data security measures that arises under the GLBA, 15 U.S.C. §§6801-6809, and its implementing regulations, 16 C.F.R. §314 (the "Safeguards Rule"), which "sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information" and "applies to the handling of customer information by all financial institutions[.]" 16 C.F.R. §314.1(a)-(b).

265. The Safeguards Rule "applies to all customer information in [a financial institution's] possession, regardless of whether such information pertains to individuals with whom [a financial institution has] a customer relationship, or pertains to the customers of other financial institutions that have provided such information to [the subject financial institution]." 16 C.F.R. §314.1(b).

266. The Safeguards Rule requires financial institutions to "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to [the financial institution's] size and complexity, the nature and scope of [the financial institution's] activities, and the sensitivity of any customer information at issue." 16 C.F.R. §314.3(a).

267. Specifically, the Safeguards Rule requires a financial institution, among other things, to:

> (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:
>
> > (1) Employee training and management;
> >
> > (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
> >
> > (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.
>
> (c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or

> otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
>
> * * *
>
> (e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program. 16 C.F.R. §314.4.

268. As alleged herein, Equifax breached its duties under the Safeguards Rule. The security program and safeguards Equifax maintained were not appropriate to Equifax's size and complexity, the nature and scope of its business, and the sensitivity of the PII of the hundreds of millions of U.S. consumers that it obtains, stores, uses, transmits, and manages. As alleged above, Equifax's security program and safeguards were not adequate to: identify reasonably foreseeable internal and external risks, assess the sufficiency of safeguards in place to control for these risks, or to detect, prevent, or respond to a data breach. In particular, Equifax's security program and safeguards were inadequate to evaluate and adjust to events that would have a material impact on Equifax's information security program, such as the numerous prior data breaches that other retailers and Equifax itself had experienced and the notification to Equifax that an identified vulnerability in a software program it utilized would make Equifax particularly susceptible to a data breach.

269. Equifax's violation of the Safeguards Rule constitutes negligence per se.

270. The Safeguards Rule "applies to all customer information in [Equifax's] possession, regardless of whether such information pertains to individuals with whom [it has] a customer relationship, or ***pertains to the customers of other financial institutions [like many of the FI Plaintiffs and members of the Class] that have provided such information to [Equifax]***." 16 C.F.R. §314.1(b) [Emphasis added]. FI Plaintiffs and the Class are "financial institutions" under the GLBA and therefore are expressly within the scope of persons the GLBA's implementing regulations were intended to protect. Furthermore, FI Plaintiffs and the Class are the entities that are required to, and did in fact, reimburse consumers whose financial accounts held with FI Plaintiffs and the Class were impacted by identity theft or other fraudulent banking activity as a result of the Equifax Data Breach. Moreover, many of the class members are credit unions, which are organized as cooperatives whose members are consumers whose PII was compromised as a result of the Equifax Data Breach.

271. Furthermore, the harm that has occurred is the type of harm the Safeguards Rule was intended to guard against. Indeed, the FTC has pursued enforcement actions against businesses which, as a result of their failure to employ

reasonable data security measures, caused the same harm suffered by FI Plaintiffs and the Class here.

272. Section 5 of the FTC Act, 15 U.S.C. §45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of not acting reasonably in the management of the data, and not using reasonable security measures to protect such data. by companies such as Equifax. FTC guidelines, publications, and consent orders described above also form the basis of Equifax's duty. In addition, individual states have enacted statutes based on the FTC Act and/or that otherwise require Equifax to act reasonably in the management of the data, and to use reasonable security measures to protect such data, as detailed herein, that also created a duty.

273. Equifax violated Section 5 of the FTC Act (and similar state statutes) by mishandling consumer data and not using reasonable measures to protect PII and Payment Card Data and by not complying with applicable industry standards. Equifax's conduct was particularly unreasonable given the nature of the business conducted by Equifax and the vast amount of PII it obtained and stored and the foreseeable consequences of a data breach at a major credit reporting agency, including specifically the immense damages that would result to consumers and financial institutions.

274. Equifax mishandled its data management and IT systems by adopting and maintaining data security measures that Equifax knew or should have known were unreasonable and inadequate to protect PII and Payment Card Data. The specific affirmative negligent acts and omissions committed by Equifax include, but are not limited to, the following:

a. Intentionally ignoring warnings about specific vulnerabilities in its systems identified by Equifax's own employees, consultants, and software vendors;

b. Maintaining (i) faulty patch management procedures, (ii) an inadequate firewall, (iii) feeble monitoring of endpoint and non-existent exfiltration monitoring, (iv) weak network segmentation, (v) inadequate monitoring and logging of network access, and (vi) insufficiently strict credentialing procedures that failed to restrict access to those with a valid purpose;

c. Refusing to timely and adequately update security certifications on key systems;

d. Storing and retaining PII in easily accessible systems rather than segregating it into locations with limited access and maximum security measures; and

e. Failing to disclose the Data Breach in a timely manner.

275. Equifax's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

276. FI Plaintiffs and the Class are within the scope of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect as they are engaged in trade and commerce and bear primary responsibility for paying for and reimbursing consumers for fraud losses and other costs associated with the compromise of PII. Moreover, many of the class members are credit unions, which are organized as cooperatives whose members are consumers.

277. Furthermore, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same type of harm suffered by FI Plaintiffs and the Class here.

278. As a direct and proximate result of Equifax's negligence per se, FI Plaintiffs and the Class have suffered and continue to suffer injury and damages as described herein.

279. Because no statutes of other states are implicated, Georgia common law applies to the negligence per se claim of FI Plaintiffs and the Class.

COUNT 3

Negligent Misrepresentation

(On behalf of FI Plaintiffs and the FI Plaintiffs Nationwide Class)

280. FI Plaintiffs repeat and reallege each and every allegation contained above as if fully set forth herein.

281. Equifax misrepresented material information to FI Plaintiffs and the Class by:

a. Misrepresenting that it would protect the confidentiality of PII, including by implementing and maintaining reasonable data security measures; and

b. Misrepresenting that it would comply with common law and statutory duties pertaining to the security of PII, including duties imposed by the GLBA, 15 U.S.C. §§6801, *et seq*., the FTC Act, 15 U.S.C. §45, the FCRA, 15 U.S.C. §1681, and other state statutes alleged herein.

282. Under Section 552 of the Restatement (Second) of Torts, adopted by the Georgia Supreme Court, an actor is liable if it negligently provides false information in the course of its business while knowing that the information will be relied upon by others.

283. By misrepresenting that it would protect the confidentiality of PII, including by implementing and maintaining reasonable data security measures, Equifax also misrepresented that its consumer data is accurate and reliable.

284. Equifax represented that the information marketed and sold to financial institutions was accurate and reliable and that Equifax utilized reasonable measures to protect the PII it maintained. Equifax's representations were material to FI Plaintiffs and Class members, given the extreme sensitivity, value, and importance of the PII maintained by Equifax; the uncertainty and disruption that would inevitably occur in the marketplace if Equifax did not adequately protect PII; and the obvious adverse consequences to FI Plaintiffs and the Class from a substantial data breach at Equifax.

285. Equifax knew that FI Plaintiffs and Class members would reasonably rely on Equifax's representations that its data systems were secure and that the PII it obtains, stores, uses, transmits, and manages was safe and reliable.

286. Equifax knew that it was entrusted with the secure handling of massive volumes of PII and Payment Card Data.

287. Equifax knew that if it failed to properly handle the PII in its possession, that FI Plaintiffs and the Class would be foremost among the victims of the resulting fraudulent banking activity.

288. Equifax knew that no rational financial institution, creditor, or individual would willingly provide PII to Equifax if they did not believe Equifax was maintaining the highest standard of data security reasonably obtainable by an institution of Equifax's size.

289. Based upon the foregoing, it can be reasonably inferred that FI Plaintiffs and the Class relied on Equifax' false representations and that Equifax knew of such reliance.

290. Because Equifax's primary product was the sale and analysis of highly sensitive PII, and because Equifax controlled the compilation of and access to such PII, FI Plaintiffs and Class members reasonably relied to their detriment on Equifax's representations that it would maintain adequate data security as well as accurate and reliable PII.

291. Had Equifax disclosed to FI Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Equifax would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Equifax held itself out as one of the three nationwide credit-reporting companies that served as trusted linchpins of the financial system and Equifax was trusted with sensitive and valuable PII regarding hundreds of millions of consumers. Equifax accepted the

responsibility of being a "trusted steward" of data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Equifax held itself out as having a special role in the financial system with a corresponding duty of trustworthiness and care, Equifax's representations were material because they were likely to deceive reasonable financial institutions, including FI Plaintiffs and the Class, about the adequacy of Equifax's data security and ability to protect the confidentiality of PII, and FI Plaintiffs and Class members acted reasonably in relying on Equifax's misrepresentations, the truth of which they could not have discovered.

292. As a direct and proximate result of Equifax's material misrepresentations, FI Plaintiffs and the Class have suffered and continue to suffer injury and damages as described herein.

293. Because no statutes of other states are implicated, Georgia common law applies to the negligence claims of FI Plaintiffs and the Class.

COUNT 4

Violation of the Georgia Deceptive Trade Practices Act, Ga. Code Ann. §§10-1-370, *et seq*.

(On Behalf of Plaintiff Peach State Federal Credit Union and the Georgia Subclass)

294. Plaintiff Peach State Federal Credit Union ("Plaintiff," for purposes of this Count), individually and on behalf of the Georgia Subclass, repeats and realleges each and every allegation contained above as if fully alleged herein.

295. The Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA"), Ga. Code Ann. §§10-1-370, et seq., prohibits deceptive trade practices in the course of a person's "business, vocation, or occupation." Ga. Code Ann. §10-1-372(a).

296. Equifax, Plaintiff, and Georgia Subclass members are "persons" within the meaning of Ga. Code Ann. §10-1-371(5).

297. Equifax engaged in deceptive trade practices in the conduct of its business, in violation of Ga. Code Ann. §10-1-372(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another; and

c. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

298. Equifax's deceptive trade practices include:

a. Unreasonably adopting and maintaining data security measures that were inadequate to protect PII and Payment Card Data, which was a direct and proximate cause of the Equifax Data Breach;

b. Ignoring foreseeable security risks, refusing to remediate identified security risks, and failing to adequately improve security measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax Data Breach;

c. Failing to comply with the common law to avoid causing foreseeable risk of harm and statutory duties pertaining to the security of PII and Payment Card Data, including duties imposed by the FTC Act, 15 U.S.C. §45, the FCRA, 15 U.S.C. §1681, and the GLBA, 15 U.S.C. §§6801, *et seq*., which was a direct and proximate cause of the Equifax Data Breach;

d. Misrepresenting that it would protect PII and Payment Card Data, including by implementing and maintaining reasonable security measures; and

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security of PII and Payment Card Data, including duties imposed by the FTC Act, 15 U.S.C. §45, the FCRA, 15 U.S.C. §1681, and the GLBA, 15 U.S.C. §§6801, *et seq*.

299. Equifax's conduct caused substantial injury to consumers and businesses and provided no benefit to consumers or competition. Equifax cut corners and minimized costs, instead placing the burden on financial institutions, like Plaintiff, to protect PII and Payment Card Data. Further, the injuries suffered by Plaintiff and the Georgia Subclass are not outweighed by any countervailing benefits to consumers or competition. And, because Equifax is solely responsible for securing its networks and protecting PII, there is no way Plaintiff and the Georgia Subclass could have known about Equifax's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Equifax's legitimate business interests, other than its conduct responsible for the Data Breach.

300. Equifax intended to mislead Plaintiff and Georgia Subclass members and induce them to rely on its misrepresentations and omissions.

301. In the course of its business, Equifax engaged in activities with a tendency or capacity to deceive.

302. Had Equifax disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, Equifax would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Equifax held itself out as one of the three nationwide credit-reporting companies that served as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable PII regarding hundreds of millions of consumers, including Plaintiff and the Georgia Subclass. Equifax accepted the responsibility of being a "trusted steward" of data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Equifax held itself out as having a special role in the financial system with a corresponding duty of trustworthiness and care, Equifax's representations were material because they were likely to deceive reasonable financial institutions about the adequacy of Equifax's data security and ability to protect the confidentiality of PII and Payment Card Data and Plaintiff and

the Georgia Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

303. As a direct and proximate result of Equifax's deceptive trade practices, Plaintiff and Georgia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages.

304. Plaintiff and Georgia Subclass members seek all relief allowed by law, including injunctive relief, and reasonable attorneys' fees and costs, under Ga. Code Ann. §10-1-373.

COUNT 5

Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 Ill. Comp. Stat. §§505/1, *et seq*.

(On Behalf of Plaintiff Consumers Cooperative Credit Union and the Illinois Subclass)

305. Plaintiff Consumers Cooperative Credit Union ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and realleges each and every allegation as contained above as if fully alleged herein.

306. The Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA"), 815 Ill. Comp. Stat. §§505/1, *et seq.*, prohibits unfair methods of competition and unfair or deceptive acts or practices in the conduct of trade or

commerce. *See* 815 Ill. Comp. Stat. §505/2. ICFA expressly provides that consideration be given to interpretations by the FTC relating to Section 5 of the Federal Trade Commission Act. *See id*.

307. Equifax is a "person" as defined by 815 Ill. Comp. Stat. §505/1(c).

308. Equifax's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. §505/1(f).

309. Plaintiff and Illinois Subclass members are a "person," as defined in 815 Ill. Comp. Stat. Ann. §505/1(c), are a "consumer," as defined in 815 Ill. Comp. Stat. Ann. §5051(e), and satisfy the consumer nexus test in that Equifax's unfair and deceptive acts and practices were directed at and impacted the market generally and/or otherwise implicate consumer protection concerns where Equifax's unfair and deceptive acts and practices have impacted at least thousands of consumers in Illinois and millions nationwide and remedying Equifax's wrongdoing through the relief requested herein would serve the interests of consumers. Furthermore, Plaintiff and the Illinois Subclass are financial institutions located in Illinois, of which there are more than 550, that extend the credit that facilitates economic growth in Illinois and that therefore rely on the integrity of the credit reporting industry.

310. Equifax advertised, offered, or sold goods or services in Illinois and therefore engaged in trade or commerce directly or indirectly affecting the people of Illinois.

311. Under ICFA the use or employment of any practice described in Section 2 of the Uniform Deceptive Trade Practices Act ("UTPA"), 815 Ill. Comp. Stat. Ann. §510/2, in the conduct of any trade or commerce is unlawful whether any person has in fact been misled, deceived, or damaged thereby.

312. Equifax engaged in deceptive trade practices in the conduct of its business, in violation of 815 Ill. Comp. Stat. §510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another; and

c. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

313. Equifax's unfair and deceptive trade practices include:

a. Unreasonably adopting and maintaining data security measures that were inadequate to protect PII, which was a direct and proximate cause of the Equifax Data Breach;

b. Ignoring foreseeable security risks, refusing to remediate identified security risks, and failing to adequately improve security measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax Data Breach;

c. Failing to comply with the common law to avoid causing foreseeable risk of harm and statutory duties pertaining to the security of PII, including duties imposed by the FTC Act, 15 U.S.C. §45, the FCRA, 15 U.S.C. §1681, the GLBA, 15 U.S.C. §§6801, *et seq*., and 815 Ill. Comp. Stat. §530/45, which was a direct and proximate cause of the Equifax Data Breach;

d. Misrepresenting that it would protect PII, including by implementing and maintaining reasonable security measures; and

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security of PII, including duties imposed by the FTC Act, 15 U.S.C. §45, the FCRA, 15 U.S.C. §1681, the GLBA, 15 U.S.C. §§6801, *et seq*., and 815 Ill. Comp. Stat. §530/45.

314. Equifax's conduct constitutes unfair methods of competition and unfair practices within the meaning of ICFA because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Equifax cut corners and minimized costs, instead placing the burden on financial institutions, like Plaintiff, to protect PII. Further, the injuries suffered by Plaintiff and the Illinois Subclass are not outweighed by any countervailing benefits to consumers or competition. And, because Equifax is solely responsible for securing its networks and protecting PII, there is no way Plaintiff and the Illinois Subclass could have known about Equifax's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Equifax's legitimate business interests, other than its conduct responsible for the Data Breach.

315. Equifax's conduct also constitutes unfair practices within the meaning of ICFA because it undermines public policy that businesses protect personal and financial information, as reflected in the FTC Act, 15 U.S.C. §45, the FCRA, 15 U.S.C. §1681, the GLBA, 15 U.S.C. §§6801, *et seq.*, and 815 Ill. Comp. Stat. §530/45.

316. Equifax intended to mislead Plaintiff and Illinois Subclass members and induce them to rely on its misrepresentations.

317. Plaintiff and the Illinois Subclass reasonably expected Equifax to maintain secure networks, adhere to industry standards, and otherwise use reasonable care to protect PII.

318. Had Equifax disclosed to Plaintiff and the Illinois Subclass that its data systems were not secure and, thus, vulnerable to attack, Equifax would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Equifax held itself out as one of the three nationwide credit reporting companies that served as trusted linchpins of the financial system and Equifax was trusted with sensitive and valuable PII regarding hundreds of millions of consumers. Equifax accepted the responsibility of being a "trusted steward" of data while keeping the inadequate state of its security controls secret from the public and financial institutions. Accordingly, because Equifax held itself out as having a special role in the financial system with a corresponding duty of trustworthiness and care, Equifax's representations were material because they were likely to deceive reasonable financial institutions about the adequacy of Equifax's data security and ability to protect the confidentiality of PII and Plaintiff and the Illinois Subclass members acted reasonably in relying on Equifax's misrepresentations, the truth of which they could not have discovered.

319. As a direct and proximate result of Equifax's unfair, unlawful, and deceptive trade practices, Plaintiff and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, monetary and non-monetary damages.

320. Plaintiff and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

COUNT 6

Violation of the Louisiana Unfair Trade Practices Act, La. Stat. Ann. §§51:1401, *et seq*.

(On Behalf of Plaintiff ASI Federal Credit Union and the Louisiana Subclass)

321. Plaintiff ASI Federal Credit Union ("Plaintiff," for purposes of this Count), individually and on behalf of the Louisiana Subclass, repeats and realleges each and every allegation contained above as if fully alleged herein.

322. The Louisiana Unfair Trade Practices and Consumer Protection Law ("LUPTA") makes unlawful "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce." La. Stat. Ann. §51:1405(A). Unfair acts are those that offend established public policy, while deceptive acts are practices that amount to fraud, deceit, or misrepresentation.

323. Equifax, Plaintiff, and the Louisiana Subclass members are "persons" within the meaning of the La. Stat. Ann. §51:1402(8).

324. Plaintiff and Louisiana Subclass members are "consumers" within the meaning of La. Stat. Ann. §51:1402(1). Plaintiff and the Louisiana Subclass are financial institutions located in Louisiana, of which there are more than 250, that extend the credit that facilitates economic growth in Louisiana and that therefore rely on the integrity of the credit reporting industry.

325. Equifax engaged in "trade" or "commerce" within the meaning of La. Stat. Ann. §51:1402(10).

326. Equifax participated in unfair and deceptive acts and practices that violated the LUTPA, including:

a. Unreasonably adopting and maintaining data security measures that were inadequate to protect PII, which was a direct and proximate cause of the Equifax Data Breach;

b. Ignoring foreseeable security risks, refusing to remediate identified security risks, and failing to adequately improve security measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax Data Breach;

c. Failing to comply with the common law to avoid causing foreseeable risk of harm and statutory duties pertaining to the security of PII, including duties imposed by the FTC Act, 15 U.S.C. §45, the FCRA, 15 U.S.C. §1681, and the GLBA, 15 U.S.C. §§6801, *et seq*., which was a direct and proximate cause of the Equifax Data Breach;

d. Misrepresenting that it would protect PII, including by implementing and maintaining reasonable security measures; and

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security of PII, including duties imposed by the FTC Act, 15 U.S.C. §45, the FCRA, 15 U.S.C. §1681, and the GLBA, 15 U.S.C. §§6801, *et seq*.

327. Equifax's conduct is not only deceptive, but also unfair within the meaning of LUTPA because it constitutes immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Equifax cut corners and minimized costs, instead placing the burden on financial institutions, like Plaintiff, to protect PII. Further, the injuries suffered by Plaintiff and the Louisiana Subclass

are not outweighed by any countervailing benefits to consumers or competition. And, because Equifax is solely responsible for securing its networks and protecting PII, there is no way Plaintiff and the Louisiana Subclass could have known about Equifax's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Equifax's legitimate business interests, other than its conduct responsible for the Data Breach.

328. Equifax's conduct is also unfair within the meaning of LUTPA because it undermines Louisiana public policy that businesses protect personal and financial information, as reflected in the FTC Act, 15 U.S.C. §45, the FCRA, 15 U.S.C. §1681, and the GLBA, 15 U.S.C. §§6801, *et seq*.

329. Equifax intended to mislead Plaintiff and Louisiana Subclass members and induce them to rely on its misrepresentations.

330. Had Equifax disclosed to Plaintiffs and Louisiana Subclass members that its data systems were not secure and, thus, vulnerable to attack, Equifax would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Equifax held itself out as one of the three nationwide credit-reporting companies that served as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable PII regarding hundreds of millions of consumers, including Plaintiff and

the Louisiana Subclass. Equifax accepted the responsibility of being a "trusted steward" of data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Equifax held itself out as having a special role in the financial system with a corresponding duty of trustworthiness and care, Equifax's representations were material because they were likely to deceive reasonable financial institutions about the adequacy of Equifax's data security and ability to protect the confidentiality of PII and Plaintiff and the Louisiana Subclass members acted reasonably in relying on Equifax's misrepresentations, the truth of which they could not have discovered.

331. As a direct and proximate result of Equifax's unfair and deceptive acts and practices, Plaintiff and Louisiana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages.

332. Plaintiff and Louisiana Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages; treble damages for Equifax's knowing violations of the LUTPA; declaratory relief; attorneys' fees; and any other relief that is just and proper.

COUNT 7

Violation of the New Mexico Unfair Practices Act, N.M. Stat. Ann. §§57-12-1, *et seq*.

(On Behalf of Plaintiff First Financial Credit Union and the New Mexico Subclass)

333. Plaintiff First Financial Credit Union ("Plaintiff," for purposes of this Count), individually and on behalf of the New Mexico Subclass, repeats and realleges each and every allegation contained as if fully alleged herein.

334. The New Mexico Unfair Practices Act ("NMUPA") N.M. Stat. Ann. §§57-12-1, *et seq.*, prohibits unfair or deceptive trade practices in the conduct of any trade or commerce. *See* N.M. Stat. Ann. §57-12-3; *see also* N.M. Stat. Ann. §57-12-2(D). The NMUPA expressly provides that consideration be given to interpretations by the FTC relating to Section 5 of the Federal Trade Commission Act. N.M. Stat. Ann. §57-12-4.

335. Equifax is a "person" as meant by N.M. Stat. Ann. §57-12-2(A).

336. Plaintiff and members of the New Mexico Subclass are a "person" as meant by N.M. Stat. Ann. §57-12-2(A). Plaintiff and the New Mexico Subclass are financial institutions located in New Mexico, of which there are more than 50, that extend the credit that facilitates economic growth in New Mexico and that therefore rely on the integrity of the credit reporting industry.

337. Equifax was engaged in "trade" and "commerce" as meant by N.M. Stat. Ann. §57-12-2(C) when engaging in the conduct alleged, directly or indirectly affecting the people of New Mexico.

338. Equifax engaged in unfair and deceptive acts and practices in connection with the sale of goods or services in the regular course of its trade or commerce, including the following:

a. Knowingly representing that its goods and services have characteristics, benefits, or qualities that they do not have, in violation of N.M. Stat. Ann. §57-12-2(D)(5); and

b. Knowingly representing that its goods and services are of a particular standard or quality when they are of another in violation of N.M. Stat. Ann. §57-12-2(D)(7).

339. Equifax's unfair and deceptive acts and practices include:

a. Unreasonably adopting and maintaining data security measures that were inadequate to protect PII, which was a direct and proximate cause of the Equifax Data Breach;

b. Ignoring foreseeable security risks, refusing to remediate identified security risks, and failing to adequately improve security measures following previous cybersecurity incidents,

which was a direct and proximate cause of the Equifax Data Breach;

c. Failing to comply with the common law to avoid causing foreseeable risk of harm and statutory duties pertaining to the security of PII, including duties imposed by the FTC Act, 15 U.S.C. §45, the FCRA, 15 U.S.C. §1681, the GLBA, 15 U.S.C. §§6801, *et seq*., and New Mexico statutes requiring protections for Social Security numbers, N.M. Stat. Ann. §57-12B-3(D), and mandating reasonable data security, N.M. Stat. Ann. §57-12C-4, which was a direct and proximate cause of the Equifax Data Breach;

d. Misrepresenting that it would protect PII, including by implementing and maintaining reasonable security measures; and

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security of PII, including duties imposed by the FTC Act, 15 U.S.C. §45, the FCRA, 15 U.S.C. §1681, the GLBA, 15 U.S.C. §§6801, *et seq*., and New Mexico statutes requiring protections for Social Security numbers, N.M.

Stat. Ann. §57-12B-3(D), and mandating reasonable data security, N.M. Stat. Ann. §57-12C-4.

340. Equifax's conduct is unfair within the meaning of NMUPA because it constitutes immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. Equifax cut corners and minimized costs, instead placing the burden on financial institutions, like Plaintiff, to protect PII. Further, the injuries suffered by Plaintiff and the New Mexico Subclass are not outweighed by any countervailing benefits to consumers or competition. And, because Equifax is solely responsible for securing its networks and protecting PII, there is no way Plaintiff and the New Mexico Subclass could have known about Equifax's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Equifax's legitimate business interests, other than its conduct responsible for the Data Breach.

341. Equifax's conduct is also unfair and unconscionable within the meaning of NMUPA because it undermines public policy that businesses protect personal and financial information, as reflected in the FTC Act, 15 U.S.C. §45, the FCRA, 15 U.S.C. §1681, the GLBA, 15 U.S.C. §§6801, *et seq*., and New Mexico

statutes requiring protections for Social Security numbers, N.M. Stat. Ann. §57-12B-3(D), and mandating reasonable data security, N.M. Stat. Ann. §57-12C-4.

342. Equifax intended to mislead Plaintiff and New Mexico Subclass members and induce them to rely on its misrepresentations.

343. Had Equifax disclosed to Plaintiff and the New Mexico Subclass that its data systems were not secure and, thus, vulnerable to attack, Equifax would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Equifax held itself out as one of the three nationwide credit reporting companies that served as trusted linchpins of the financial system and Equifax was trusted with sensitive and valuable PII regarding hundreds of millions of consumers. Equifax accepted the responsibility of being a "trusted steward" of data while keeping the inadequate state of its security controls secret from the public and financial institutions. Accordingly, because Equifax held itself out as having a special role in the financial system with a corresponding duty of trustworthiness and care, Equifax's representations were material because they were likely to deceive reasonable financial institutions about the adequacy of Equifax's data security and ability to protect the confidentiality of PII and Plaintiff and the New Mexico Subclass members acted reasonably in relying on Equifax's misrepresentations, the truth of which they could not have discovered.

344. As a direct and proximate result of Equifax's unfair, deceptive, and unconscionable trade practices, Plaintiff and New Mexico Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages.

345. Plaintiff and New Mexico Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages or statutory damages of $100 (whichever is greater), treble damages or statutory damages of $300 (whichever is greater), and reasonable attorneys' fees and costs.

COUNT 8

Violation of New York General Business Law, N.Y. Gen. Bus. Law §§349, *et seq.*

(On Behalf of Plaintiffs The Summit Federal Credit Union and Hudson River Community Credit Union and the New York Subclass)

346. Plaintiffs The Summit Federal Credit Union and Hudson River Community Credit Union ("Plaintiff," for purposes of this Count), individually and on behalf of the New York Subclass, repeat and reallege each and every allegation contained above as if fully alleged herein.

347. New York General Business Law §349 ("GBL §349") prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service" in New York. Plaintiff and the New York Subclass

are financial institutions located in New York, of which there are more than 400, which extend the credit that facilitates economic growth in New York and that therefore rely on the integrity of the credit reporting industry.

348. Equifax engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of GBL §349, including:

a. Unreasonably adopting and maintaining data security measures that were inadequate to protect PII, which was a direct and proximate cause of the Equifax Data Breach;

b. Ignoring foreseeable security risks, refusing to remediate identified security risks, and failing to adequately improve security measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax Data Breach;

c. Failing to comply with the common law to avoid causing foreseeable risk of harm and statutory duties pertaining to the security of PII, including duties imposed by the FCRA, 15 U.S.C. §1681, which was a direct and proximate cause of the Equifax Data Breach;

d. Misrepresenting that it would protect PII, including by implementing and maintaining reasonable security measures; and

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security of PII, including duties imposed by the FCRA, 15 U.S.C. §1681.

349. Equifax's conduct caused substantial injury to consumers and businesses and provided no benefit to consumers or competition. Equifax cut corners and minimized costs, instead placing the burden on financial institutions, like Plaintiff, to protect PII. Further, the injuries suffered by Plaintiff and the New York Subclass are not outweighed by any countervailing benefits to consumers or competition. And, because Equifax is solely responsible for securing its networks and protecting PII, there is no way Plaintiff and the New York Subclass could have known about Equifax's inadequate data security practices or avoided the injuries they sustained. There were reasonably available alternatives to further Equifax's legitimate business interests, other than its conduct responsible for the Data Breach.

350. Had Equifax disclosed to Plaintiff and the New York Subclass that its data systems were not secure and, thus, vulnerable to attack, Equifax would have been unable to continue in business and it would have been forced to adopt

reasonable data security measures and comply with the law. Instead, Equifax held itself out as one of the three nationwide credit reporting companies that served as trusted linchpins of the financial system and Equifax was trusted with sensitive and valuable PII regarding hundreds of millions of consumers. Equifax accepted the responsibility of being a "trusted steward" of data while keeping the inadequate state of its security controls secret from the public and financial institutions. Accordingly, because Equifax held itself out as having a special role in the financial system with a corresponding duty of trustworthiness and care, Equifax's representations were material because they were likely to deceive reasonable financial institutions about the adequacy of Equifax's data security and ability to protect the confidentiality of PII and Plaintiff and the New York Subclass members acted reasonably in relying on Equifax's misrepresentations, the truth of which they could not have discovered.

351. Equifax's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the millions of New Yorkers affected by the Equifax Data Breach. Equifax's unlawful acts and practices complained of herein affect consumers at large and the public interest, including the millions of New Yorkers and more than 400 banks and credit unions headquartered in New York, affected by the Equifax Data Breach. Equifax's deceptive acts and practices were likely to and did in fact deceive the public at large

and reasonable consumers, including FI Plaintiffs and Class members, regarding the security and accuracy of the PII it obtains, stores, uses, transmits, and manages. Equifax's violations present a continuing risk to FI Plaintiffs and Class members, as well as to the general public.

352. Therefore, FI Plaintiffs bring this action on behalf of themselves and Class members for the public benefit in order to promote the public interests in the provision of truthful, fair information that enables financial institutions that extend credit to consumers and the public at large to make informed decisions related to the security of PII, and to protect the public from Equifax's unlawful acts and practices.

353. As a direct and proximate result of Equifax's deceptive and unlawful acts and practices, Plaintiff and New York Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages.

354. Plaintiff and New York Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $50 (whichever is greater), treble damages, injunctive relief, and attorney's fees and costs.

COUNT 9

Declaratory and Equitable Relief

(On Behalf of the FI Plaintiffs and the FI Plaintiffs Nationwide Class and the Association Plaintiffs)

355. Plaintiffs repeat and reallege each and every allegation contained above as if fully set forth herein.

356. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and that violate the terms of the federal and state statutes described in this complaint.

357. An actual controversy has arisen in the wake of Equifax's Data Breach regarding its common law and other duties to reasonably safeguard its customers' PII and Payment Card Data. Plaintiffs allege that Equifax's data security measures were inadequate and remain inadequate. Equifax denies these allegations. Furthermore, Plaintiffs continue to suffer injury and damages as described herein.

358. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Equifax continues to owe a legal duty to act reasonably in managing consumer data and to secure PII and Payment Card

Data under, *inter alia*, the common law, GLBA, Section 5 of the FTC Act, the FCRA, and the state statutes alleged to herein;

b. Equifax continues to breach its legal duty by actively mishandling consumer data and failing to employ reasonable measures to secure PII and Payment Card Data; and

c. Equifax's ongoing breaches of its legal duty continue to cause Plaintiffs harm.

359. The Court should also issue corresponding injunctive relief requiring Equifax to employ adequate security protocols consistent with industry standards to protect PII and Payment Card Data. This injunction should direct Equifax to implement data security procedures, protocols, and measures that are in accordance with industry best practices and that are appropriate for the size and complexity of Equifax's business and the sensitivity of the PII it obtains, stores, uses, transmits and manages. More specifically, this injunction should, among other things, direct Equifax to:

a. Implement procedures to provide for timely and proper patching of all servers with appropriate security-specific system patches;

b. Implement procedures to timely and properly update security certificates

c. Install an appropriate firewall;

d. Implement strong network segmentation;

e. Provide for sufficient logging and monitoring of network access, exfiltration monitoring, and whitelisting;

f. Enhance endpoint and email security;

g. Strengthen credentialing procedures and restrict access to PII to those with a valid purpose;

h. Install all upgrades recommended by manufacturers of security software and firewalls used by Equifax;

i. Engage third party auditors to test its systems for weakness and upgrade any such weakness found;

j. Train and audit its data security personnel regarding any new or modified procedures and how to respond to a data breach; and

k. Regularly test its systems for security vulnerabilities, consistent with industry standards, and upgrade any vulnerabilities identified.

360. If an injunction is not issued, Plaintiffs will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Equifax, which is a real possibility given the continued missteps taken by Equifax described herein,

including using its official corporate communications to send affected consumers to phishing sites. Indeed, Equifax was hit with a separate data breach in March 2017 that apparently did nothing to motivate it to discover the other massive data breach going on at the same time.[171] The risk of another such breach is real, immediate, and substantial. If another breach at Equifax occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct. In particular, FI Plaintiffs will be subject to reputational harm and the loss of goodwill resulting from the customer confusion and anxiety that will occur when another data breach and identity theft impacts them.

361. The hardship to FI Plaintiffs and the Class if an injunction does not issue exceeds the hardship to Equifax if an injunction is issued. Among other things, if another massive data breach occurs at Equifax, FI Plaintiffs and the Classes will likely incur millions of dollars in damages and the credit reporting system on which FI Plaintiffs and the Class rely could collapse. On the other hand, the cost to Equifax of complying with an injunction by employing reasonable data security measures is

[171] Mark Coppock, *Equifax Confirms It Suffered A Separate Data Breach In March*, DIGITAL TRENDS (Oct. 3, 2017), https://www.digitaltrends.com /computing/equifax-data-breach-affects-143-million-americans/.

relatively minimal, and Equifax has a pre-existing legal obligation to employ such measures.

362. Issuance of the requested injunction will serve the public interest by preventing another data breach at Equifax, thus eliminating the injuries that would result to Plaintiffs, the Classes, and the potentially millions of consumers whose confidential information would be compromised.

COUNT 10

Reasonable Attorneys' Fees and Expenses of Litigation, Ga. Code Ann. §13-6-11

(On Behalf of the FI Plaintiffs and the Association Plaintiffs)

363. Plaintiffs repeat and reallege each and every allegation contained above as if fully set forth herein.

364. Defendants through their actions alleged and described herein acted in bad faith, were stubbornly litigious, or caused Plaintiffs unnecessary trouble and expense with respect to the transaction or events underlying this litigation.

365. As alleged above, Equifax's senior management ignored specific warnings that its systems were vulnerable to attack and refused to take the necessary steps to adequately protect consumer data. As a direct result of Equifax's weak cybersecurity measures, between at least May and July 2017, hackers stole the highly sensitive PII of approximately 147.9 million U.S. consumers as well as Payment

Card Data. As further alleged above, the Equifax Data Breach was a direct consequence of Equifax's deliberate decisions not to adopt recommended data security measures, decisions that left PII vulnerable. Equifax's data security deficiencies were so significant that the hackers' activities went undetected for at least two months. During that time, the hackers had unfettered access to exfiltrate likely hundreds of millions of lines of consumer data. Had Equifax adopted reasonable data security measures, it could have prevented the Data Breach.

366. As further described above, FI Plaintiffs and the Class have been injured, suffering financial losses directly attributable to the Data Breach. Specifically, because their customers' PII and/or Payment Card Data was compromised in the Data Breach, FI Plaintiffs and the Class have incurred direct out-of-pocket costs resulting from Defendants' action.

367. Had Equifax adopted reasonable data security measures, it could have prevented the Data Breach. Instead, Equifax did not place a high priority on data security, took a careless approach to patching systems – including the ones responsible for causing the Data Breach – and failed to comply with industry standards of care to protect against known threats to its sensitive cache of PII.

368. Plaintiffs therefore request that their claim for recovery of expenses of litigation and attorneys' fees be submitted to the jury, and that the Court enter a

Judgment awarding their expenses of litigation and attorneys' fees pursuant to O.C.G.A. §13-6-11.

PRAYER FOR RELIEF

WHEREFORE, FI Plaintiffs, individually and on behalf of the Classes, and the Association Plaintiffs (as appropriate to the specific claim they have brought) respectfully request that the Court:

A. Certify the Classes and appoint FI Plaintiffs and FI Plaintiffs' counsel to represent the Classes;

B. Enter a monetary judgment in favor of FI Plaintiffs and the Classes to compensate them for the injuries they have suffered and will continue to suffer, together with pre-judgment and post-judgment interest and treble damages and penalties where appropriate;

C. Enter a declaratory judgment as described herein and corresponding injunctive relief requiring Equifax to employ adequate data security protocols consistent with industry standards to protect PII and Payment Card Data;

D. Grant the injunctive relief requested herein;

E. Award Plaintiffs and the Classes reasonable attorneys' fees and costs of suit, as allowed by law; and

F. Award such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all claims so triable.

Respectfully submitted this 20th day of March, 2019.

/s Joseph P. Guglielmo
Joseph P. Guglielmo
Erin Green Comite
Carey Alexander
Margaret B. Ferron
SCOTT+SCOTT
ATTORNEYS AT LAW LLP
230 Park Avenue, 17th Floor
New York, NY 10169
Tel.: 212-223-6444
Fax: 212-223-6334
jguglielmo@scott-scott.com
ecomite@scott-scott.com
calexander@scott-scott.com
mferron@scott-scott.com

Gary F. Lynch
Jamisen A. Etzel
Kevin Tucker
CARLSON LYNCH SWEET KILPELA & CARPENTER, LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, Pennsylvania 15222
Tel.: 412-322-9243
Fax: 412-231-0246
glynch@carlsonlynch.com
jetzel@carlsonlynch.com

ktucker@carlsonlynch.com

Co-Lead Counsel for the Financial Institution Plaintiff Class

Craig A. Gillen
Ga. Bar No.
Anthony C. Lake
Ga. Bar No. 431149
GILLEN WITHERS & LAKE, LLC
3490 Piedmont Road, N.E.
One Securities Centre, Suite 1050
Atlanta, GA 30305
Tel.: 404-842-9700
Fax: 404-842-9750
cgillen@gwllawfirm.com
aclake@gwllawfirm.com

MaryBeth V. Gibson
THE FINLEY FIRM, P.C.
3535 Piedmont Road
Building 14, Suite 230
Atlanta, GA 30305
Tel.: 404-320-9979
Fax: 404-320-9978
mgibson@thefinleyfirm.com

Ranse M. Partin
CONLEY GRIGGS PARTIN, LLP
Building One, Suite 300
4200 Northside Parkway, NW
Atlanta, GA 30327
Tel.: 404-467-1155
Fax: 404-467-1166
ranse@conleygriggs.com

Co-Liaison Counsel for the Financial Institution Plaintiff Class

Arthur M. Murray
Stephen B. Murray, Sr.
Caroline W. Thomas
MURRAY LAW FIRM
650 Poydras Street, Suite 2150
New Orleans, LA 70130
Tel.: 504-525-8100
Fax: 504-584-5249
amurray@murray-lawfirm.com
smurray@murray-lawfirm.com
cthomas@murray-lawfirm.com

Stacey P. Slaughter
Michael Ram
ROBINS KAPLAN LLP
800 LaSalle Avenue Suite 2800
Minneapolis, MN 612-349-8500
Tel.: 612-349-8500
Fax: 612-339-4181
sslaughter@robinskaplan.com
mram@robinskaplan.com

Charles H. Van Horn
BERMAN FINK VANHORN P.C.
3475 Piedmont Road, Suite 1100
Atlanta, GA 30305
Tel.: 404-261-7711
Fax: 404-233-1943
cvanhorn@bfvlaw.com

Allen Carney
Joseph Henry Bates
CARNEY BATES & PULLIAM, PLLC
519 W. 7th Street
Little Rock, AR 72201
Tel.: 501-312-8500

Fax: 501-312-8505
acarney@cbplaw.com
hbates@cbplaw.com

Bryan L. Bleichner
CHESTNUT CAMBRONNE PA
17 Washington Avenue North
Suite 300
Minneapolis, MN 55401
Tel.: 612-339-7300
Fax: 612-336-2940
bbleichner@chestnutcambronne.com

Karen Hanson Riebel
Kate M. Baxter-Kauf
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Ave. S., Suite 2200
Minneapolis, MN 55401
Tel.: 612-339-6900
Fax: 612-339-0981
khriebel@locklaw.com
kmbaxter-kauf@locklaw.com

Karen S. Halbert
Michael L. Roberts
Jana K. Law
ROBERTS LAW FIRM, PA
20 Rahling Circle
P.O. Box 241790
Little Rock, AR 72223
Tel.: 501-821-5575
Fax: 501-821-4474
karenhalbert@robertslawfirm.us
mikeroberts@robertslawfirm.us
janalaw@robertslawfirm.us

Brian C. Gudmundson

ZIMMERMAN REED LLP
1100 IDS Center, 80 South 8th Street
Minneapolis, MN 55402
Tel.: 612-341-0400
Fax: 612-341-0844
brian.gudmundson@zimmreed.com

Steering Committee for the Financial Institution Plaintiff Class

Richard L. Coffman
THE COFFMAN LAW FIRM
First City Building
505 Orleans St., Fifth Floor
Beaumont, TX 77701
Tel.: 409-833-7700
Fax: 866-835-8250
Email: rcoffman@coffmanlawfirm.com

Reginald L. Snyder
DYE SNYDER, LLP
260 Peachtree St. NW, Suite 502
Atlanta, GA 30303
Tel.: 678-974-8360
Fax: 404-393-3872
Email: rsnyder@dyesnyder.com

Mary C. Turke
Samuel J. Strauss
TURKE & STRAUSS, LLP
Suite 201
613 Williamson Street
Madison, WI 53703
Tel.: 608-237-1775
Fax: 608-509-4423
mary@turkestrauss.com
sam@turkestrauss.com

David A. Reed
REED & JOLLY, PLLC
3711 Millpond Court
Fairfax, VA 22033
Tel.: 703-675-9578
David@reedandjolly.com

Charles Barrett
NEAL & HARWELL, PLC
1201 Demonbreun Suite 1000
Nashville, TN 37203
Tel.: 615-238-3647
Fax: 615-726-0573
cbarrett@nealharwell.com

Robert C. Khayat, Jr.
THE KHAYAT LAW FIRM
Georgia Bar No. 416981
75 Fourteenth Street, N.E.
Suite 2750
Atlanta, Georgia 30309
Tel.: 404-978-2750
Fax: 404-978-2901
rkhayat@khayatlawfirm.com

David M. Cohen
COMPLEX LAW GROUP, LLC
Ga. Bar No. 173503
40 Powder Springs Street
Marietta, GA 30064
Tel.: 770-200-3100
Fax: 770-200-3101
dcohen@complexlaw.com

Additional Counsel for Plaintiffs

CERTIFICATE OF SERVICE

The undersigned hereby certifies that, on this 20th day of March, 2019, the undersigned electronically filed the foregoing filing using the CM/ECF system, which will automatically send email notification of such filing to all attorneys of record in this case.

/s Joseph P. Guglielmo
Joseph P. Guglielmo
SCOTT+SCOTT
ATTORNEYS AT LAW LLP
230 Park Avenue, 17th Floor
New York, NY 10169
Tel.: 212-223-6444
Fax: 212-223-6334
jguglielmo@scott-scott.com