IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

In re: Equifax, Inc. Customer Data Security Breach Litigation	)	MDL Docket No. 2800
	)	Case No.: 1:17-md-2800-TWT
	)	
	)	**CONSUMER ACTIONS**
	)	

CONSOLIDATED CONSUMER CLASS ACTION COMPLAINT

"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."

Richard F. Smith, Equifax's former Chief Executive Officer
October 3, 2017

Amy E. Keller
DICELLO LEVITT & CASEY LLC
Ten North Dearborn Street
Eleventh Floor
Chicago, Illinois 60602

Kenneth S. Canfield
DOFFERMYRE SHIELDS CANFIELD & KNOWLES, LLC
1355 Peachtree Street, N.E. Suite 1900
Atlanta, Georgia 30309

Norman E. Siegel
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112

Consumer Plaintiffs' Co-Lead Counsel
Other Counsel Identified on Signature Pages

TABLE OF CONTENTS

INTRODUCTION.....1

JURISDICTION AND VENUE.....4

NAMED PLAINTIFFS.....5

DEFENDANTS AND THEIR RELEVANT CORPORATE STRUCTURE...70

STATEMENT OF FACTS.....75

The Importance of Consumer Credit in the U.S. Economy 75

Equifax Compiles Massive Amounts of Consumer Information 78

Equifax Recognized the Importance of Data Security 85

Equifax Has a History of Inadequate Data Security Practices 94

The Equifax Data Breach.....102

Equifax Discovers the Data Breach.....107

Equifax's Inadequate Data Security Practices.....112

Equifax's Botched Public Disclosure and Response to the Breach 119

Equifax Recommends Implementing Credit Freezes 133

Reactions to the Data Breach.....140

Aftermath of the Breach: Consequences for Consumers and the Economy 145

CLASS ACTION ALLEGATIONS 152

CHOICE OF LAW FOR NATIONWIDE CLAIMS 160

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT 1.....161
VIOLATION OF THE FAIR CREDIT REPORTING ACT
15 U.S.C. §§ 1681, *et seq*.

COUNT 2.....167
NEGLIGENCE

COUNT 3 175
NEGLIGENCE *PER SE*

COUNT 4 176
GEORGIA FAIR BUSINESS PRACTICES ACT

COUNT 5 186
UNJUST ENRICHMENT

COUNT 6 189
DECLARATORY JUDGMENT

CLAIMS ON BEHALF OF THE EQUIFAX CONTRACT SUBCLASS

COUNT 7 192
BREACH OF CONTRACT

COUNT 8 194
BREACH OF IMPLIED CONTRACT

CLAIMS ON BEHALF OF THE FCRA DISCLOSURE SUBCLASS

COUNT 9 197
VIOLATION OF THE FAIR CREDIT REPORTING ACT
15 U.S.C. § 1681g(a)

CLAIMS ON BEHALF OF THE ALABAMA SUBCLASS

COUNT 10 199
ALABAMA DECEPTIVE TRADE PRACTICES ACT
Ala. Code §§ 8-19-1, *et seq*.

CLAIMS ON BEHALF OF THE ALASKA SUBCLASS

COUNT 11 205
PERSONAL INFORMATION PROTECTION ACT
Alaska Stat. §§ 45.48.010, *et seq*.

COUNT 12 207
ALASKA CONSUMER PROTECTION ACT
Alaska Stat. §§ 45.50.471, *et seq*.

CLAIMS ON BEHALF OF THE ARIZONA SUBCLASS

COUNT 13 212
ARIZONA CONSUMER FRAUD ACT
A.R.S. §§ 44-1521, *et seq*.

CLAIMS ON BEHALF OF THE ARKANSAS SUBCLASS

COUNT 14 216
ARKANSAS DECEPTIVE TRADE PRACTICES ACT
A.C.A. §§ 4-88-101, *et seq*.

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT 15 222
CALIFORNIA CUSTOMER RECORDS ACT
Cal. Civ. Code §§ 1798.80, *et seq*.

COUNT 16 224
CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code §§ 17200, *et seq*.

COUNT 17 230
CALIFORNIA CONSUMER LEGAL REMEDIES ACT
Cal. Civ. Code §§ 1750, *et seq*.

CLAIMS ON BEHALF OF THE COLORADO SUBLCASS

COUNT 18 233
COLORADO SECURITY BREACH NOTIFICATION ACT
Colo. Rev. Stat. §§ 6-1-716, *et seq*.

COUNT 19 235
COLORADO CONSUMER PROTECTION ACT
Colo. Rev. Stat. §§ 6-1-101, *et seq*.

CLAIMS ON BEHALF OF THE CONNECTICUT SUBCLASS

COUNT 20 240
BREACH OF SECURITY REGARDING COMPUTERIZED DATA
C.G.S.A. § 36a-701b

CLAIMS ON BEHALF OF THE DELAWARE SUBCLASS

COUNT 21 242
DELAWARE COMPUTER SECURITY BREACH ACT
6 Del. Code Ann. §§ 12B-102, *et seq*.

COUNT 22 243
DELAWARE CONSUMER FRAUD ACT
6 Del. Code §§ 2513, *et seq*.

CLAIMS ON BEHALF OF THE DISTRICT OF COLUMBIA SUBCLASS

COUNT 23 248
DISTRICT OF COLUMBIA CONSUMER SECURITY BREACH NOTIFICATION ACT
D.C. Code §§ 28-3851, *et seq*.

COUNT 24 250
DISTRICT OF COLUMBIA CONSUMER PROTECTION PROCEDURES ACT
D.C. Code §§ 28-3904, *et seq*.

CLAIMS ON BEHALF OF THE FLORIDA SUBCLASS

COUNT 25 255
FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT
Fla. Stat. §§ 501.201, *et seq*.

CLAIMS ON BEHALF OF THE GEORGIA SUBCLASS

COUNT 26 259
GEORGIA SECURITY BREACH NOTIFICATION ACT
O.C.G.A. §§ 10-1-912, *et seq*.

COUNT 27 261
GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT
O.C.G.A. §§ 10-1-370, *et seq*.

CLAIMS ON BEHALF OF THE HAWAII SUBCLASS

COUNT 28 266
HAWAII SECURITY BREACH NOTIFICATION ACT
Haw. Rev. Stat. §§ 487N-1, *et seq*.

COUNT 29 267
HAWAII UNFAIR PRACTICES AND UNFAIR COMPETITION ACT
Haw. Rev. Stat. §§ 480-1, *et seq*.

COUNT 30 271
HAWAII UNIFORM DECEPTIVE TRADE PRACTICE ACT
Haw. Rev. Stat. §§ 481A-3, *et seq*.

CLAIMS ON BEHALF OF THE IDAHO SUBCLASS

COUNT 31 275
IDAHO CONSUMER PROTECTION ACT
Idaho Code §§ 48-601, *et seq*.

CLAIMS ON BEHALF OF THE ILLINOIS SUBCLASS

COUNT 32 279
ILLINOIS PERSONAL INFORMATION PROTECTION ACT
815 Ill. Comp. Stat. §§ 530/10(a), *et seq*.

COUNT 33 281
ILLINOIS CONSUMER FRAUD ACT
815 Ill. Comp. Stat. §§ 505, *et seq*.

COUNT 34 285
ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT
815 Ill. Comp. Stat. §§ 510/2, *et seq*.

CLAIMS ON BEHALF OF THE INDIANA SUBCLASS

COUNT 35 290
INDIANA DECEPTIVE CONSUMER SALES ACT
Ind. Code §§ 24-5-0.5-1, *et seq*.

CLAIMS ON BEHALF OF THE IOWA SUBCLASS

COUNT 36 300
PERSONAL INFORMATION SECURITY BREACH PROTECTION LAW
Iowa Code § 715C.2

COUNT 37 301
IOWA PRIVATE RIGHT OF ACTION FOR CONSUMER FRAUDS ACT
Iowa Code § 714H

CLAIMS ON BEHALF OF THE KANSAS SUBCLASS

COUNT 38 305
PROTECTION OF CONSUMER INFORMATION
Kan. Stat. Ann. §§ 50-7a02(a), *et seq*.

COUNT 39 307
KANSAS CONSUMER PROTECTION ACT
K.S.A. §§ 50-623, *et seq*.

CLAIMS ON BEHALF OF THE KENTUCKY SUBCLASS

COUNT 40 313
KENTUCKY COMPUTER SECURITY BREACH NOTIFICATION ACT
Ky. Rev. Stat. Ann. §§ 365.732, *et seq*.

COUNT 41 314
KENTUCKY CONSUMER PROTECTION ACT
Ky. Rev. Stat. §§ 367.110, *et seq*.

CLAIMS ON BEHALF OF THE LOUISIANA SUBCLASS

COUNT 42 318
DATABASE SECURITY BREACH NOTIFICATION LAW
La. Rev. Stat. Ann. §§ 51:3074(A), *et seq*.

COUNT 43 320
LOUISIANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW
La. Rev. Stat. Ann. §§ 51:1401, *et seq*.

CLAIMS ON BEHALF OF THE MAINE SUBCLASS

COUNT 44 325
MAINE UNFAIR TRADE PRACTICES ACT
5 Me. Rev. Stat. §§ 205, 213, *et seq*.

COUNT 45 329
MAINE UNIFORM DECEPTIVE TRADE PRACTICES ACT
10 Me. Rev. Stat. §§ 1212, *et seq*.

CLAIMS ON BEHALF OF THE MARYLAND SUBCLASS

COUNT 46 334
MARYLAND PERSONAL INFORMATION PROTECTION ACT
Md. Comm. Code §§ 14-3501, *et seq*.

COUNT 47 337
MARYLAND SOCIAL SECURITY NUMBER PRIVACY ACT
Md. Comm. Code §§ 14-3401, *et seq*.

COUNT 48 338
MARYLAND CONSUMER PROTECTION ACT
Md. Comm. Code §§ 13-301, *et seq*.

CLAIMS ON BEHALF OF THE MASSACHUSETTS SUBCLASS

COUNT 49 344
MASSACHUSETTS CONSUMER PROTECTION ACT
Mass. Gen. Laws Ann. Ch. 93A, §§ 1, *et seq*.

CLAIMS ON BEHALF OF THE MICHIGAN SUBCLASS

COUNT 50 349
MICHIGAN IDENTITY THEFT PROTECTION ACT
Mich. Comp. Laws Ann. §§ 445.72, *et seq*.

COUNT 51 351
MICHIGAN CONSUMER PROTECTION ACT
Mich. Comp. Laws Ann. §§ 445.903, *et seq*.

CLAIMS ON BEHALF OF THE MINNESOTA SUBCLASS

COUNT 52 355
MINNESOTA CONSUMER FRAUD ACT
Minn. Stat. §§ 325F.68, *et seq.* and Minn. Stat. §§ 8.31, *et seq*.

COUNT 53 359
MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT
Minn. Stat. §§ 325D.43, *et seq*.

CLAIMS ON BEHALF OF THE MISSISSIPPI SUBCLASS

COUNT 54 364
MISSISSIPPI CONSUMER PROTECTION ACT
Miss. Code §§ 75-24-1, *et seq*.

CLAIMS ON BEHALF OF THE MISSOURI SUBCLASS

COUNT 55 370
MISSOURI MERCHANDISE PRACTICES ACT
Mo. Rev. Stat. §§ 407.010, *et seq*.

CLAIMS ON BEHALF OF THE MONTANA SUBCLASS

COUNT 56 374
COMPUTER SECURITY BREACH LAW
Mont. Code Ann. §§ 30-14-1704(1), *et seq*.

COUNT 57 376
MONTANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION ACT
M.C.A. §§ 30-14-101, *et seq*.

CLAIMS ON BEHALF OF THE NEBRASKA SUBCLASS

COUNT 58 380
NEBRASKA CONSUMER PROTECTION ACT
Neb. Rev. Stat. §§ 59-1601, *et seq*.

COUNT 59 384
NEBRASKA UNIFORM DECEPTIVE TRADE PRACTICES ACT
Neb. Rev. Stat. §§ 87-301, *et seq*.

CLAIMS ON BEHALF OF THE NEVADA SUBCLASS

COUNT 60 389
NEVADA DECEPTIVE TRADE PRACTICES ACT
Nev. Rev. Stat. Ann. §§ 598.0903, *et seq*.

CLAIMS ON BEHALF OF THE NEW HAMPSHIRE SUBCLASS

COUNT 61 394
NOTICE OF SECURITY BREACH
N.H. Rev. Stat. Ann. §§ 359-C:20(I)(A), *et seq*.

COUNT 62 396
NEW HAMPSHIRE CONSUMER PROTECTION ACT
N.H.R.S.A. §§ 358-A, *et seq*.

CLAIMS ON BEHALF OF THE NEW JERSEY SUBCLASS

COUNT 63 400
NEW JERSEY CUSTOMER SECURITY BREACH
DISCLOSURE ACT
N.J. Stat. Ann. §§ 56:8-163, *et seq*.

COUNT 64 402
NEW JERSEY CONSUMER FRAUD ACT
N.J. Stat. Ann. §§ 56:8-1, *et seq*.

CLAIMS ON BEHALF OF THE NEW MEXICO SUBCLASS

COUNT 65 406
NEW MEXICO UNFAIR PRACTICES ACT
N.M. Stat. Ann. §§ 57-12-2, *et seq*.

CLAIMS ON BEHALF OF THE NEW YORK SUBCLASS

COUNT 66 411
INFORMATION SECURITY BREACH AND NOTIFICATION ACT
N.Y. Gen. Bus. Law § 899-aa

COUNT 67 413
NEW YORK GENERAL BUSINESS LAW
N.Y. Gen. Bus. Law §§ 349, *et seq*.

CLAIMS ON BEHALF OF THE NORTH CAROLINA SUBCLASS

COUNT 68 416
NORTH CAROLINA IDENTITY THEFT PROTECTION ACT
N.C. Gen. Stat. §§ 75-60, *et seq*.

COUNT 69 418
NORTH CAROLINA UNFAIR TRADE PRACTICES ACT
N.C. Gen. Stat. Ann. §§ 75-1.1, *et seq*.

CLAIMS ON BEHALF OF THE NORTH DAKOTA SUBCLASS

COUNT 70 422
NOTICE OF SECURITY BREACH FOR PERSONAL INFORMATION
N.D. Cent. Code §§ 51-30-02, *et seq*.

COUNT 71 424
NORTH DAKOTA UNLAWFUL SALES OR ADVERTISING ACT
N.D. Cent. Code §§ 51-15-01, *et seq*.

CLAIMS ON BEHALF OF THE OHIO SUBCLASS

COUNT 72 429
OHIO CONSUMER SALES PRACTICES ACT
Ohio Rev. Code §§ 1345.01, *et seq*.

COUNT 73 434
OHIO DECEPTIVE TRADE PRACTICES ACT
Ohio Rev. Code §§ 4165.01, *et seq*.

CLAIMS ON BEHALF OF THE OKLAHOMA SUBCLASS

COUNT 74 438
OKLAHOMA CONSUMER PROTECTION ACT
Okla. Stat. Tit. 15, §§ 751, *et seq*.

CLAIMS ON BEHALF OF THE OREGON SUBCLASS

COUNT 75 443
OREGON CONSUMER IDENTITY THEFT PROTECTION ACT
Or. Rev. Stat. §§ 646A.604(1), *et seq*.

COUNT 76 445
OREGON UNLAWFUL TRADE PRACTICES ACT
Or. Rev. Stat. §§ 646.608, *et seq*.

CLAIMS ON BEHALF OF THE PENNSYLVANIA SUBCLASS

COUNT 77 451
PENNSYLVANIA UNFAIR TRADE PRACTICES AND
CONSUMER PROTECTION LAW
73 Pa. Cons. Stat. §§ 201-2 & 201-3, *et seq*.

CLAIMS ON BEHALF OF THE PUERTO RICO SUBCLASS

COUNT 78 456
CITIZEN INFORMATION ON DATA BANKS SECURITY ACT
P.R. Laws Ann. tit. 10, §§ 4051, *et seq*.

CLAIMS ON BEHALF OF THE RHODE ISLAND SUBCLASS

COUNT 79 457
RHODE ISLAND DECEPTIVE TRADE PRACTICES ACT
R.I. Gen. Laws §§ 6-13.1, *et seq*.

CLAIMS ON BEHALF OF THE SOUTH CAROLINA SUBCLASS

COUNT 80 462
SOUTH CAROLINA DATA BREACH SECURITY ACT
S.C. Code Ann. §§ 39-1-90, *et seq*.

COUNT 81 464
SOUTH CAROLINA UNFAIR TRADE PRACTICES ACT
S.C. Code Ann. §§ 39-5-10, *et seq*.

CLAIMS ON BEHALF OF THE SOUTH DAKOTA SUBCLASS

COUNT 82 471
SOUTH DAKOTA DECEPTIVE TRADE PRACTICES AND CONSUMER PROTECTION LAW
S.D. Codified Laws §§ 37-24-1, *et seq*.

CLAIMS ON BEHALF OF THE TENNESSEE SUBCLASS

COUNT 83 477
TENNESSEE PERSONAL CONSUMER INFORMATION RELEASE ACT
Tenn. Code Ann. §§ 47-18-2107, *et seq*.

COUNT 84 478
TENNESSEE CONSUMER PROTECTION ACT
Tenn. Code Ann. §§ 47-18-101, *et seq*.

CLAIMS ON BEHALF OF THE TEXAS SUBCLASS

COUNT 85 486
DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT
Texas Bus. & Com. Code §§ 17.41, *et seq*.

CLAIMS ON BEHALF OF THE UTAH SUBCLASS

COUNT 86 494
UTAH CONSUMER SALES PRACTICES ACT
Utah Code §§ 13-11-1, *et seq*.

CLAIMS ON BEHALF OF THE VERMONT SUBCLASS

COUNT 87 502
VERMONT CONSUMER FRAUD ACT
Vt. Stat. Ann. Tit. 9, §§ 2451, *et seq*.

CLAIMS ON BEHALF OF THE VIRGIN ISLANDS SUBCLASS

COUNT 88 508
IDENTITY THEFT PREVENTION ACT
V.I. Code tit. 14 §§ 2208, *et seq*.

COUNT 89 510
VIRGIN ISLANDS CONSUMER FRAUD
AND DECEPTIVE BUSINESS PRACTICES ACT
V.I. Code tit. 12A, §§ 301, *et seq*.

COUNT 90 516
VIRGIN ISLANDS CONSUMER PROTECTION LAW
V.I. Code tit. 12A, §§101, *et seq*.

CLAIMS ON BEHALF OF THE VIRGINIA SUBCLASS

COUNT 91 522
VIRGINIA PERSONAL INFORMATION BREACH
NOTIFICATION ACT
Va. Code. Ann. §§ 18.2-186.6, *et seq*.

COUNT 92 524
VIRGINIA CONSUMER PROTECTION ACT
Va. Code Ann. §§ 59.1-196, *et seq*.

CLAIMS ON BEHALF OF THE WASHINGTON SUBCLASS

COUNT 93 530
WASHINGTON DATA BREACH NOTICE ACT
Wash. Rev. Code §§ 19.255.010, *et seq*.

COUNT 94 532
WASHINGTON CONSUMER PROTECTION ACT
Wash. Rev. Code Ann. §§ 19.86.020, *et seq*.

CLAIMS ON BEHALF OF THE WEST VIRGINIA SUBCLASS

COUNT 95 536
WEST VIRGINIA CONSUMER CREDIT AND PROTECTION ACT
W. Va. Code §§46A-6-101, *et seq*.

CLAIMS ON BEHALF OF THE WISCONSIN SUBCLASS

COUNT 96 545
NOTICE OF UNAUTHORIZED ACQUISITION OF PERSONAL INFORMATION
Wis. Stat. §§ 134.98(2), *et seq*.

COUNT 97 547
WISCONSIN DECEPTIVE TRADE PRACTICES ACT
Wis. Stat. § 100.18

CLAIMS ON BEHALF OF THE WYOMING SUBCLASS

COUNT 98 552
COMPUTER SECURITY BREACH; NOTICE TO AFFECTED PERSONS
Wyo. Stat. Ann. §§ 40-12-502(a), *et seq*.

CLAIM FOR RECOVERY OF EXPENSES OF LITIGATION

COUNT 99 554
O.C.G.A. § 13-6-11

REQUEST FOR RELIEF 554

DEMAND FOR JURY TRIAL 556

The individual consumer Plaintiffs identified below (collectively, "Plaintiffs"), individually and on behalf of the Classes defined below of similarly situated persons, allege the following against Defendants Equifax Inc., Equifax Information Services LLC ("EIS"), and Equifax Consumer Services LLC ("ECS") (collectively, "Equifax" or "Defendants"), based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

INTRODUCTION

1. Equifax plays a central role in the modern American economy, collecting and selling vast amounts of data about the most important details of consumers' financial lives. That data—names, birthdates, Social Security numbers, credit card information, drivers' license numbers, and more—contains the keys that unlock a consumer's identity and is relied upon by third-parties to make major financial decisions affecting almost all Americans. Equifax understood it had an enormous responsibility to protect the data it collected and assured the public that: "At Equifax, the security of our customers' information is paramount." But, as its former CEO has acknowledged, Equifax has not lived up to that responsibility or fulfilled its public assurances to protect Americans' confidential information.

The individual consumer plaintiffs identified below (collectively, "Plaintiffs"), individually and on behalf of the Classes defined below of similarly situated persons, allege the following against Defendants Equifax Inc., Equifax Information Services LLC ("EIS"), and Equifax Consumer Services LLC ("ECS") (collectively, "Equifax" or "Defendants"), based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

INTRODUCTION

1. Equifax plays a central role in the modern American economy, collecting and selling vast amounts of data about the most important details of consumers' financial lives. That data—names, birthdates, Social Security numbers, credit card information, drivers' license numbers, and more—contains the keys that unlock a consumer's identity and is relied upon by third parties to make major financial decisions affecting almost all Americans. Equifax understood it had an enormous responsibility to protect the data it collected and assured the public that: "At Equifax, the security of our customers' information is paramount." But, as its former CEO has acknowledged, Equifax has not lived up to that responsibility or fulfilled its public assurances to protect Americans' confidential information.

2. On September 7, 2017, Equifax announced that it was subject to one of the largest data breaches in our nation's history. Taking advantage of glaring weaknesses and vulnerabilities in the company's data security systems, hackers stole the personal and financial information of nearly 150 million Americans from mid-May through the end of July, 2017. During that entire two and one-half month period, Equifax failed to detect the hackers' presence, notice the massive amounts of data that were being exfiltrated from its databases, or take any steps to investigate the numerous other red flags that should have warned the company about what was happening.

3. Equifax has attributed the breach to a low-level employee's failure to install a necessary software patch. While that employee's negligence may have created the door through which the hackers first entered, the breach was in fact the inevitable result of Equifax's systemic incompetence and a longstanding, lackluster approach to data security that permeated the company's culture from the top down. Indeed, Equifax's cavalier attitude about data security persisted despite warnings by outside cybersecurity experts, the occurrence of other data breaches at Equifax, and numerous high-profile data breaches at other major American corporations, all of which should have alerted Equifax of the need to revamp and enhance its woefully inadequate data security practices.

4. The severity of this breach is unprecedented, affecting almost half of the American population. Nearly all of the victims had no prior relationship with Equifax, and there is no mechanism to opt-out of Equifax's collection and sale of this data. The hackers obtained at least 146.6 million names, 146.6 million dates of birth, 145.5 million Social Security numbers, 99 million addresses, 17.6 million driver's license numbers, 209,000 credit card numbers, and 97,500 tax identification numbers. Using this information, identity thieves can create fake identities, fraudulently obtain loans and tax refunds, and destroy a consumer's credit-worthiness—the very thing Equifax exists to assess and report. And because Social Security numbers do not expire and are almost impossible to change, thieves will be able to do so for years to come. As one knowledgeable analyst noted soon after the breach was announced: "On a scale of 1 to 10 in terms of risk to consumers, this is a 10."

5. Since the Equifax breach occurred, unwitting consumers across the United States have been victims of identity theft and sustained resulting economic loss. Millions have incurred costs to mitigate the risk, such as paying for "credit freezes" or credit monitoring products. Regardless of whether they have yet to incur out-of-pocket losses, all of the 147.9 million Americans whose information was stolen in the breach remain subject to a pervasive, substantial and imminent

risk of identity theft and fraud, a risk that will continue so long as Social Security numbers have such a critical role in consumers' financial lives.

6. This class action is brought by 96 individuals from across the United States on behalf of all natural persons victimized by the breach to redress the damage that they have suffered and to obtain appropriate equitable relief to mitigate the risk that Equifax will allow another breach in the future. Plaintiffs and the nationwide class they seek to represent assert claims for Equifax's violation of the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. §§ 1681, *et seq.*, negligence, negligence *per se*, violation of Georgia's consumer protection statute, unjust enrichment, and for a declaratory judgment. Plaintiffs also assert claims on behalf of themselves and various subclasses described below for other FCRA violations, breach of contract and implied contract, and violation of numerous state statutes relating to consumer protection, data security, and data breach notification.

JURISDICTION AND VENUE

7. This Consolidated Complaint is intended to serve as a superseding complaint as to all other complaints consolidated in this multidistrict litigation that were filed on behalf of natural persons, and to serve for all purposes as the operative pleading for the Classes defined below. As set forth herein, this Court

has general jurisdiction over Equifax and original jurisdiction over Plaintiffs' claims.

8. This Court has federal question subject-matter jurisdiction pursuant to 28 U.S.C. § 1331, because Plaintiffs allege that Equifax violated the FCRA.

9. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, and Equifax is a citizen of a State different from that of at least one Class member. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

10. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because Equifax's principal place of business is located in this District and substantial parts of the events or omissions giving rise to the claims occurred in the District. Venue is also proper in the Atlanta Division because Equifax is located here and the causes of action arose here.

NAMED PLAINTIFFS

11. The Plaintiffs identified below bring this action on behalf of themselves and those similarly situated both across the United States and within their State or Territory of residence. As with the rest of the 147.9 million victims of

the Equifax data breach, Equifax through its actions described herein leaked, disbursed, and furnished their valuable Personal Information (as defined below) to unknown cyber criminals, thus causing them present, immediate, imminent, and continuing increased risk of harm.

12. As used throughout this Complaint, "Personal Information" is defined as all information exposed by the Equifax data breach, including all or any part or combination of name, address, birth date, Social Security number, driver's license information (any part of license number, state, home address, dates of issuance or expiration), telephone number, email address, tax identification number, credit card number, or dispute documents with personally identifying information (such as images of government-issued identifications).

ALABAMA

13. Plaintiff Germany Davis is a resident and citizen of the State of Alabama and her Personal Information was compromised in the Equifax data breach. Plaintiff Davis verified through Equifax's data breach response website that her Personal Information was compromised. Before the announcement of the breach, Plaintiff Davis purchased Equifax Complete credit monitoring from Equifax. Plaintiff Davis did not receive the benefit of her purchase because Equifax's inadequate data security practices subjected Plaintiff Davis to the precise

type of harm that she was seeking to protect against. Equifax also violated its agreement with Plaintiff Davis to safeguard the privacy and security of her information. Plaintiff Davis would not have purchased this product had she known of Equifax's inadequate data security practices. In addition, as a result of the breach, Plaintiff Davis spent time and effort searching for and implementing applications on her phone, as well as online services, to alert her to fraud and/or identity theft. Given the highly-sensitive nature of the information stolen, Plaintiff Davis remains at a substantial and imminent risk of future harm.

14. Plaintiff Sanjay Rajput is a resident and citizen of the State of Alabama, and his Personal Information was compromised in the Equifax data breach. Plaintiff Rajput verified through Equifax's data breach response website that his Personal Information was compromised. As a direct result of the breach, Plaintiff Rajput spent time and money purchasing credit freezes with Experian and TransUnion in order to mitigate possible harm. Before the announcement of the breach, Plaintiff Rajput also purchased Equifax ID Patrol credit monitoring from Equifax. Plaintiff Rajput did not receive the benefit of his purchase because Equifax's inadequate data security practices subjected Plaintiff Rajput to the precise type of harm that he was seeking to protect against. Equifax also violated its agreement with Plaintiff Rajput to safeguard the privacy and security of his

information. Plaintiff Rajput would not have purchased this product had he known of Equifax's inadequate data security practices. In addition, as a result of the breach, Plaintiff Rajput spent time and effort making multiple telephone calls to Equifax regarding the breach, monitoring his financial accounts, searching for fraudulent activity, and reviewing his credit report. Given the highly-sensitive nature of the information stolen, Plaintiff Rajput remains at a substantial and imminent risk of future harm.

ALASKA

15. Plaintiff Michael Aaron Bishop is a resident and citizen of the State of Alaska, and his Personal Information was compromised in the Equifax data breach. Plaintiff Bishop verified through Equifax's data breach response website that his Personal Information was compromised. Before the announcement of the breach, Plaintiff Bishop purchased credit monitoring with identity theft protection from Equifax. Plaintiff Bishop did not receive the benefit of his purchase because Equifax's inadequate data security practices subjected Plaintiff Bishop to the precise type of harm that he was seeking to protect against. Equifax also violated its agreement with Plaintiff Bishop to safeguard the privacy and security of his information. Plaintiff Bishop would not have purchased this product had he known of Equifax's inadequate data security practices. In addition, as a result of the

breach, Plaintiff Bishop paid to maintain his credit monitoring services from TransUnion and Experian in order to mitigate possible harm and spent time and effort monitoring his accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Bishop remains at a substantial and imminent risk of future harm.

ARIZONA

16. Plaintiff Thomas W. Hannon is a resident and citizen of the State of Arizona, and his Personal Information was compromised in the Equifax data breach. Plaintiff Hannon verified through Equifax's data breach response website that his Personal Information was compromised. As a direct result of the breach, Plaintiff Hannon spent time and money purchasing identity theft protection from LifeLock in order to mitigate possible harm. In addition, as a result of the breach, Plaintiff Hannon spent time and effort monitoring his financial accounts and searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Hannon remains at a substantial and imminent risk of future harm.

17. Plaintiff Benjamin Sanchez is a resident and citizen of the State of Arizona, and his Personal Information was compromised in the Equifax data breach. Plaintiff Sanchez verified through Equifax's data breach response website

that his Personal Information was compromised. As a result of the breach, Plaintiff Sanchez has suffered identity theft in the form of an unauthorized credit card opened in his name using his Personal Information. As a result of this identity theft, Plaintiff Sanchez spent time and effort disputing the unauthorized credit card application. In addition, as a result of the breach, Plaintiff Sanchez spent time and effort searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Sanchez remains at a substantial and imminent risk of future harm.

18. Plaintiff David Sands is a resident and citizen of the State of Arizona, and his Personal Information was compromised in the Equifax data breach. Plaintiff Sands verified through Equifax's data breach response website that his Personal Information was compromised. Before the announcement of the breach, Plaintiff Sands purchased identity theft protection from Equifax. Plaintiff Sands did not receive the benefit of his purchase because Equifax's inadequate data security practices subjected Plaintiff Sands to the precise type of harm that he was seeking to protect against. Equifax also violated its agreement with Plaintiff Sands to safeguard the privacy and security of his information. Plaintiff Sands would not have purchased this product had he known of Equifax's inadequate data security practices. In addition, as a result of the breach, Plaintiff Sands spent time and effort

monitoring his financial accounts and searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Sands remains at a substantial and imminent risk of future harm.

ARKANSAS

19. Plaintiff Richard Whittington II is a resident and citizen of the State of Arkansas, and his Personal Information was compromised in the Equifax data breach. Plaintiff Whittington verified through Equifax's data breach response website that his Personal Information was compromised. Before the announcement of the breach, Plaintiff Whittington purchased Equifax Complete Premier Plan credit monitoring from Equifax. Plaintiff Whittington did not receive the benefit of his purchase because Equifax's inadequate data security practices subjected Plaintiff Whittington to the precise type of harm that he was seeking to protect against. Equifax also violated its agreement with Plaintiff Whittington to safeguard the privacy and security of his information. Plaintiff Whittington would not have purchased this product had he known of Equifax's inadequate data security practices. Given the highly-sensitive nature of the information stolen, Plaintiff Whittington remains at a substantial and imminent risk of future harm.

20. Plaintiff Brenda King is a resident and citizen of the State of Arkansas, and her Personal Information was compromised in the Equifax data

breach. Plaintiff King verified through Equifax's data breach response website that her Personal Information was compromised. Given the highly-sensitive nature of the information stolen, Plaintiff King remains at a substantial and imminent risk of future harm.

CALIFORNIA

21. Plaintiff Grace Cho is a resident and citizen of the State of California, and her Personal Information was compromised in the Equifax data breach. Plaintiff Cho verified through Equifax's data breach response website that her Personal Information was compromised. As a result of the breach, Plaintiff Cho has suffered identity theft in the form of unauthorized accounts opened in her name and using her Personal Information with a wireless phone provider and department store in order to make fraudulent purchases. In addition, other attempts were made to use Plaintiff Cho's Personal Information to open unauthorized credit accounts at a retail warehouse club and another department store. As a result of this identity theft, Plaintiff Cho spent time and effort contacting representatives to dispute and close the unauthorized accounts, filing a police report, and contacting the credit card companies and credit bureaus. In addition, as a result of the breach, Plaintiff Cho spent time and effort monitoring her financial accounts and searching for additional fraudulent activity. On September 1, 2017, Plaintiff Cho requested a

consumer report from Equifax. This report failed to inform Plaintiff Cho of the breach or potential harm she would suffer as a consequence of the breach. Given the highly-sensitive nature of the information stolen, Plaintiff Cho remains at a substantial and imminent risk of future harm.

22. Plaintiff Miche' Sharpe is a resident and citizen of the State of California, and her Personal Information was compromised in the Equifax data breach. Plaintiff Sharpe verified through Equifax's data breach response website that her Personal Information was compromised. As a result of the breach, Plaintiff Sharpe has suffered identity theft in the form of an unauthorized account and credit card opened in her name and using her Personal Information through an online retailer, and an unauthorized credit account applied for in her name and using her Personal Information through a major financial institution. As a result of this identity theft, Plaintiff Sharpe spent time and effort contacting the companies to dispute and close the unauthorized accounts, filing a police report, and filing complaints with state and federal agencies, including consumer regulatory agencies. Also as a direct result of the breach, Plaintiff Sharpe spent time and money purchasing credit monitoring from Amica Insurance in order to mitigate possible harm and time and effort searching for fraudulent activity. Given the

highly-sensitive nature of the information stolen, Plaintiff Sharpe remains at a substantial and imminent risk of future harm.

23. Plaintiff Andrew Galpern is a resident and citizen of the State of California, and his Personal Information was compromised in the Equifax data breach. Plaintiff Galpern verified through Equifax's data breach response website that his Personal Information was compromised. As a direct result of the breach, Plaintiff Galpern spent time and money purchasing credit freezes from Experian and TransUnion in order to mitigate possible harm. In addition, as a result of the breach, Plaintiff Galpern spent time and effort attempting to contact Equifax, monitoring his financial accounts, and searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Galpern remains at a substantial and imminent risk of future harm.

24. Plaintiff Nathan Alan Turner is a resident and citizen of the State of California, and his Personal Information was compromised in the Equifax data breach. Plaintiff Turner verified through Equifax's data breach response website that his Personal Information was compromised. As a direct result of the breach, Plaintiff Turner spent time and money purchasing credit monitoring from the United Services Automobile Association in order to mitigate possible harm. In addition, as a result of the breach, Plaintiff Turner spent time and effort reviewing

his bank statements and credit reports searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Turner remains at a substantial and imminent risk of future harm.

COLORADO

25. Plaintiff Nancy Rae Browning is a resident and citizen of the State of Colorado, and her Personal Information was compromised in the Equifax data breach. Plaintiff Browning verified through Equifax's data breach response website that her Personal Information was compromised. As a result of the breach, Plaintiff Browning has suffered identity theft in the form of unauthorized credit cards and unauthorized credit inquiries made in her name and using her Personal Information. As a result of this identity theft, Plaintiff Browning spent time and effort resolving the issues with the credit card company. In addition, as a result of the breach, Plaintiff Browning spent time and effort searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Browning remains at a substantial and imminent risk of future harm.

26. Plaintiff Alvin Alfred Kleveno Jr. is a resident and citizen of the State of Colorado, and his Personal Information was compromised in the Equifax data breach. Plaintiff Kleveno verified through Equifax's data breach response website that his Personal Information was compromised. In addition, Plaintiff Kleveno

received notice directly from Equifax through the mail that a debit card Plaintiff Kleveno previously used to unfreeze his credit with Equifax was compromised in the breach. As a result of the breach, Plaintiff Kleveno experienced unauthorized charges on this same debit card and spent time and effort contesting the fraudulent charges with his credit union, cancelling the card, and traveling to the credit union to obtain a replacement card. In addition, as a result of the breach, Plaintiff Kleveno spent time and effort monitoring his financial accounts for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Kleveno remains at a substantial and imminent risk of future harm.

CONNECTICUT

27. Plaintiff Cheryl Ann Tafas is a resident and citizen of the State of Connecticut, and her Personal Information was compromised in the Equifax data breach. Plaintiff Tafas verified through Equifax's data breach response website that her Personal Information was compromised. As a direct result of the breach, Plaintiff Tafas spent time and money purchasing credit freezes with Equifax, Experian, and TransUnion, and paid to maintain her credit monitoring services from Bank of America in order to mitigate possible harm. In addition, as a result of the breach, Plaintiff Tafas spent time and effort monitoring her financial accounts and searching for fraudulent activity. Given the highly-sensitive nature of the

information stolen, Plaintiff Tafas remains at a substantial and imminent risk of future harm.

DELAWARE

28. Plaintiff Janelle Ferrell is a resident and citizen of the State of Delaware, and her Personal Information was compromised in the Equifax data breach. Plaintiff Ferrell verified through Equifax's data breach response website that her Personal Information was compromised. As a result of the breach, Plaintiff Ferrell spent time and effort monitoring her financial accounts and searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Ferrell remains at a substantial and imminent risk of future harm.

DISTRICT OF COLUMBIA

29. Plaintiff Rodd Santomauro is a resident and citizen of the District of Columbia, and his Personal Information was compromised in the Equifax data breach. Plaintiff Santomauro verified through Equifax's data breach response website that his Personal Information was compromised. As a direct result of the breach, Plaintiff Santomauro spent time and money purchasing credit protection services from LifeLock in order to mitigate possible harm. Given the highly-sensitive nature of the information stolen, Plaintiff Santomauro remains at a substantial and imminent risk of future harm.

30. Plaintiff Kathleen Holly is a resident and citizen of the District of Columbia, and her Personal Information was compromised in the Equifax data breach. Plaintiff Holly verified through Equifax's data breach response website that her Personal Information was compromised. Before the announcement of the breach, Plaintiff Holly purchased Equifax Credit Watch Gold credit monitoring from Equifax. Plaintiff Holly did not receive the benefit of her purchase because Equifax's inadequate data security practices subjected Plaintiff Holly to the precise type of harm that she was seeking to protect against. Equifax also violated its agreement with Plaintiff Holly to safeguard the privacy and security of her information. Plaintiff Holly would not have purchased this product had she known of Equifax's inadequate data security practices. In addition, as a result of the breach, Plaintiff Holly spent time and effort monitoring her financial accounts and additional consumer accounts for fraudulent activity, which required her to spend numerous hours on the phone with banks and retailers. Plaintiff Holly also paid to maintain an insurance rider for identity theft protection in order to mitigate possible harm. Given the highly-sensitive nature of the information stolen, Plaintiff Holly remains at a substantial and imminent risk of future harm.

FLORIDA

31. Plaintiff Gregg Podalsky is a resident and citizen of the State of Florida, and his Personal Information was compromised in the Equifax data breach. Plaintiff Podalsky verified through Equifax's data breach response website that his Personal Information was compromised. As a direct result of the breach, Plaintiff Podalsky spent time and money purchasing identity theft protection from LegalShield and paid to maintain identity theft protection services from LifeLock in order to mitigate possible harm. In addition, as a result of the breach, Plaintiff Podalsky spent time and effort contacting his financial institutions to prevent fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Podalsky remains at a substantial and imminent risk of future harm.

32. Plaintiff Jennifer J. Tweeddale is a resident and citizen of the State of Florida, and her Personal Information was compromised in the Equifax data breach. Plaintiff Tweeddale verified through Equifax's data breach response website that her Personal Information was compromised. As a result of the breach, Plaintiff Tweeddale has suffered identity theft in the form of unauthorized accounts opened in her name and using her Personal Information. As a result of this identity theft, Plaintiff Tweeddale spent time and effort disputing the unauthorized accounts. Also as a result of the fraudulent accounts on her credit report, Plaintiff

Tweeddale's credit score dropped approximately 79 points. Also as a direct result of the breach, Plaintiff Tweeddale spent time and money purchasing credit monitoring from Experian in order to mitigate possible harm. In addition, as a result of the breach, Plaintiff Tweeddale spent time and effort monitoring her financial accounts and searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Tweeddale remains at a substantial and imminent risk of future harm.

33. Plaintiff Maria Martucci is a resident and citizen of the State of Florida, and her Personal Information was compromised in the Equifax data breach. Plaintiff Martucci verified through Equifax's data breach response website that her Personal Information was compromised. As a direct result of the breach, Plaintiff Martucci spent time and money purchasing credit freezes from TransUnion and Experian, and paid to maintain her credit monitoring from TransUnion in order to mitigate possible harm. After freezing her credit, Plaintiff Martucci subsequently paid to unfreeze her credit with Experian and TransUnion. Plaintiff Martucci received notice directly from Equifax through the mail that her debit card used to purchase credit reports from Equifax was compromised in the breach. As a result of the breach, Plaintiff Martucci experienced unauthorized charges on this same debit card. As a result of this fraud, Plaintiff Martucci spent

time and effort disputing the unauthorized charges with her bank. In addition, as a result of the breach, Plaintiff Martucci spent time and effort searching for additional fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Martucci remains at a substantial and imminent risk of harm.

GEORGIA

34. Plaintiff Wanda Paulo is a resident and citizen of the State of Georgia, and her Personal Information was compromised in the Equifax data breach. Plaintiff Paulo verified through Equifax's data breach response website that her Personal Information was compromised. As a direct result of the breach, Plaintiff Paulo spent time and money purchasing credit freezes from Equifax, TransUnion, and Experian in order to mitigate possible harm. Plaintiff Paulo subsequently paid to unfreeze and refreeze her credit with TransUnion and Experian. Given the highly-sensitive nature of the information stolen, Plaintiff Paulo remains at a substantial and imminent risk of future harm.

35. Plaintiff Justin O'Dell is a resident and citizen of the State of Georgia, and his Personal Information was compromised in the Equifax data breach. Plaintiff O'Dell verified through Equifax's data breach response website that his Personal Information was compromised. As a direct result of the breach, Plaintiff O'Dell spent time and money purchasing credit monitoring services from Experian

in order to mitigate possible harm. In addition, as a result of the breach, Plaintiff O'Dell spent time and effort monitoring his financial accounts. Given the highly-sensitive nature of the information stolen, Plaintiff O'Dell remains at a substantial and imminent risk of future harm.

36. Plaintiff Michael Chase is a resident and citizen of the State of Georgia, and his Personal Information was compromised in the Equifax data breach. Plaintiff Chase verified through Equifax's data breach response website that his Personal Information was compromised. As a direct result of the breach, Plaintiff Chase spent time and money purchasing credit freezes from Equifax, TransUnion, and Experian, and paid to maintain his annual credit monitoring subscription with Experian in order to mitigate possible harm. In addition, as a result of the breach, Plaintiff Chase spent time and effort attempting to contact Equifax to obtain additional information regarding the breach. Given the highly-sensitive nature of the information stolen, Plaintiff Chase remains at a substantial and imminent risk of future harm.

37. Plaintiff John Simmons II is a resident and citizen of the State of Georgia, and his Personal Information was compromised in the Equifax data breach. Plaintiff Simmons verified through Equifax's data breach response website that his Personal Information was compromised. As a result of the breach, Plaintiff

Simmons has suffered identity theft in the form of unauthorized accounts opened in his name and using his Personal Information, and has had creditors contact him about outstanding balances on those accounts. As a result of this identity theft, Plaintiff Simmons spent time and effort contacting his bank and the companies with which the unauthorized accounts were opened to close the unauthorized accounts, filing a police report regarding the unauthorized accounts, contacting Experian to remove the fraudulent accounts from his credit report, and placing a fraud alert on his credit report through Experian to flag any new accounts opened in his name. Also as a result of the fraudulent accounts on his credit report, Plaintiff Simmons' credit score dropped, which affected him in that it delayed his ability to obtain a home loan. Given the highly-sensitive nature of the information stolen, Plaintiff Simmons remains at a substantial and imminent risk of future harm.

38. Plaintiff Sylvia Patterson is a resident and citizen of the State of Georgia, and her Personal Information was compromised in the Equifax data breach. Plaintiff Patterson verified through Equifax's data breach response website that her Personal Information was compromised. As a result of the breach, Plaintiff Patterson has suffered identity theft in the form of unauthorized accounts and unauthorized credit cards opened in her name and using her Personal Information.

As a result of this identity theft, Plaintiff Patterson spent time and effort corresponding with creditors and LifeLock attempting to close the unauthorized accounts, filing a police report regarding the identity theft, obtaining a credit report from Experian to determine whether her credit score was impacted by the unauthorized accounts, and placing credit freezes with Equifax, TransUnion, and Experian. Plaintiff Patterson also subsequently paid to maintain her annual credit monitoring subscription with LifeLock in order to mitigate possible harm. In addition, as a result of the breach, Plaintiff Patterson spent time and effort contacting the Internal Revenue Service regarding the identity theft and marking her tax account with an identity theft indicator in order to mitigate possible additional harm. Given the highly-sensitive nature of the information stolen, Plaintiff Patterson remains at a substantial and imminent risk of future harm.

HAWAII

39. Plaintiff Bruce Pascal is a resident and citizen of the State of Hawaii, and his Personal Information was compromised in the Equifax data breach. Plaintiff Pascal verified through Equifax's data breach response website that his Personal Information was compromised. Given the highly-sensitive nature of the information stolen, Plaintiff Pascal remains at a substantial and imminent risk of future harm.

IDAHO

40. Plaintiff Brett D. Lemmons is a resident and citizen of the State of Idaho, and his Personal Information was compromised in the Equifax data breach. Plaintiff Lemmons verified through Equifax's data breach response website that his Personal Information was compromised. As a result of the breach, Plaintiff Lemmons has suffered identity theft in the form of an unauthorized loan opened in his name and using his Personal Information. As a result of this identity theft, Plaintiff Lemmons spent time and effort making telephone calls, filing a police report, and filing reports with regulators. Also as a direct result of the breach, Plaintiff Lemmons spent time and money purchasing credit monitoring from LifeLock and credit freezes from Experian and TransUnion in order to mitigate possible harm. In addition, as a result of the breach, Plaintiff Lemmons spent time and effort monitoring his financial accounts and searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Lemmons remains at a substantial and imminent risk of future harm.

ILLINOIS

41. Plaintiff Eva Hitchcock is a resident and citizen of the State of Illinois, and her Personal Information was compromised in the Equifax data breach. Plaintiff Hitchcock verified through Equifax's data breach response

website that her Personal Information was compromised. As a direct result of the breach, Plaintiff Hitchcock spent time and money purchasing identity theft protection services from LifeLock in order to mitigate possible harm. Given the highly-sensitive nature of the information stolen, Plaintiff Hitchcock remains at a substantial and imminent risk of future harm.

42. Plaintiff Kim Strychalski is a resident and citizen of the State of Illinois, and her Personal Information was compromised in the Equifax data breach. Plaintiff Strychalski verified through Equifax's data breach response website that her Personal Information was compromised. As a direct result of the breach, Plaintiff Strychalski spent time and money purchasing credit freezes from TransUnion and Experian in order to mitigate possible harm. Given the highly-sensitive nature of the information stolen, Plaintiff Strychalksi remains at a substantial and imminent risk of future harm.

INDIANA

43. Plaintiff James David Sharp is a resident and citizen of the State of Indiana, and his Personal Information was compromised in the Equifax data breach. Plaintiff Sharp verified through Equifax's data breach response website that his Personal Information was compromised. As a result of the breach, Plaintiff Sharp spent time and effort reviewing his credit reports to monitor for fraudulent

activity. Given the highly-sensitive nature of the information stolen, Plaintiff Sharp remains at a substantial and imminent risk of future harm.

44. Plaintiff Larry Frazier is a resident and citizen of the State of Indiana, and his Personal Information was compromised in the Equifax data breach. Plaintiff Frazier verified through Equifax's data breach response website that his Personal Information was compromised. As a result of the breach, Plaintiff Frazier has suffered identity theft in the form of an unauthorized credit card and loans opened in his name using his Personal Information. As a result of this identity theft, Plaintiff Frazier spent time and effort disputing the unauthorized credit card application and loans. In addition, as a result of the breach, Plaintiff Frazier spent time and effort searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Frazier remains at a substantial and imminent risk of future harm.

IOWA

45. Plaintiff Thomas E. Greenwood is a resident and citizen of the State of Iowa, and his Personal Information was compromised in the Equifax data breach. Plaintiff Greenwood verified through Equifax's data breach response website that his Personal Information was compromised. Given the highly-

sensitive nature of the information stolen, Plaintiff Greenwood remains at a substantial and imminent risk of future harm.

KANSAS

46. Plaintiff Amie Louise Smith is a resident and citizen of the State of Kansas, and her Personal Information was compromised in the Equifax data breach. Plaintiff Smith verified through Equifax's data breach response website that her Personal Information was compromised. As a result of the breach, Plaintiff Smith has suffered identity theft in the form of fraudulent accounts opened in her name and using her Personal Information through a wireless phone provider. As a result of this identity theft, Plaintiff Smith spent time and effort speaking with representatives from the wireless phone provider, filing a police report regarding the incident, and monitoring her credit history. Also as a direct result of the breach, Plaintiff Smith spent time and money purchasing credit monitoring services from Experian in order to mitigate possible harm. Given the highly-sensitive nature of the information stolen, Plaintiff Smith remains at a substantial and imminent risk of future harm.

47. Plaintiff Mark Carr is a resident and citizen of the State of Kansas, and his Personal Information was compromised in the Equifax data breach. Plaintiff Carr verified through Equifax's data breach response website that his

Personal Information was compromised. As a direct result of the breach, Plaintiff Carr spent time and effort monitoring his financial accounts for fraudulent activity and ensuring that the credit freezes he previously implemented with Equifax, Experian, and TransUnion were still in place. Given the highly-sensitive nature of the information stolen, Plaintiff Carr remains at a substantial and imminent risk of future harm.

KENTUCKY

48. Plaintiff Bob Helton is a resident and citizen of the State of Kentucky, and his Personal Information was compromised in the Equifax data breach. Plaintiff Helton verified through Equifax's data breach response website that his Personal Information was compromised. As a result of the breach, Plaintiff Helton has suffered identity theft in the form of unauthorized credit cards being applied for and opened in his name and using his Personal Information. As a result of this identity theft, Plaintiff Helton spent time and effort disputing the unauthorized accounts with his bank and filing a police report. Also as a direct result of the breach, Plaintiff Helton spent time and money purchasing credit monitoring and identity theft protection services from LifeLock in order to mitigate possible harm. In addition, as a result of the breach, Plaintiff Helton spent time and effort monitoring his financial accounts and searching for fraudulent activity. Given the

highly-sensitive nature of the information stolen, Plaintiff Helton remains at a substantial and imminent risk of future harm.

49. Plaintiff Robert Benson is a resident and citizen of the State of Kentucky, and his Personal Information was compromised in the Equifax data breach. Plaintiff Benson verified through Equifax's data breach response website that his Personal Information was compromised. As a direct result of the breach, Plaintiff Benson spent time and money purchasing credit monitoring and identity theft protection from LifeLock in order to mitigate possible harm. In addition, as a result of the breach, Plaintiff Benson spent time and effort monitoring his financial accounts and searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Benson remains at a substantial and imminent risk of future harm.

LOUISIANA

50. Plaintiff Cheyra Acklin-Davis is a resident and citizen of the State of Louisiana, and her Personal Information was compromised in the Equifax data breach. Plaintiff Acklin-Davis verified through Equifax's data breach response website that her Personal Information was compromised. As a result of the breach, Plaintiff Acklin-Davis suffered identity theft when an unauthorized individual was added to her auto insurance policy. As a result of this identity theft, Plaintiff

Acklin-Davis spent time and effort contacting her insurance company to have the unauthorized individual removed from her policy and spent money on her policy premiums, which increased after the identity theft occurred. Given the highly-sensitive nature of the information stolen, Plaintiff Acklin-Davis remains at a substantial and imminent risk of future harm.

51. Plaintiff Jasmine Guess is a resident and citizen of the State of Louisiana, and her Personal Information was compromised in the Equifax data breach. Plaintiff Guess verified through Equifax's data breach response website that her Personal Information was compromised. As a result of the breach, Plaintiff Guess has suffered identity theft in the form of unauthorized claims made through her insurance company. Plaintiff Guess also experienced unauthorized charges through her wireless phone provider for replacement cellular phones that she never requested. As a result of this identity theft, Plaintiff Guess spent time and effort contacting and working with her insurance company and cellular phone provider to address the fraudulent activity. Also as a direct result of the breach, Plaintiff Guess spent time and money enrolling in and purchasing credit monitoring from Experian in order to mitigate possible harm. Given the highly-sensitive nature of the information stolen, Plaintiff Guess remains at a substantial and imminent risk of future harm.

MAINE

52. Plaintiff Michele Renee Archambault is a resident and citizen of the State of Maine, and her Personal Information was compromised in the Equifax data breach. Plaintiff Archambault verified through Equifax's data breach response website that her Personal Information was compromised. As a result of the breach, Plaintiff Archambault spent time and effort searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Archambault remains at a substantial and imminent risk of future harm.

53. Plaintiff Barry Napier is a resident and citizen of the State of Maine, and his Personal Information was compromised in the Equifax data breach. Plaintiff Napier verified through Equifax's data breach response website that his Personal Information was compromised. As a result of the breach, Plaintiff Napier spent time and effort monitoring his financial accounts. Given the highly-sensitive nature of the information stolen, Plaintiff Napier remains at a substantial and imminent risk of future harm.

MARYLAND

54. Plaintiff Cathy Louise Henry is a resident and citizen of the State of Maryland, and her Personal Information was compromised in the Equifax data breach. Plaintiff Henry verified through Equifax's data breach response website

that her Personal Information was compromised. As a result of the breach, Plaintiff Henry has suffered identity theft in the form of an unknown individual changing the address, email, and phone number associated with one of her credit cards without her consent. As a result of this identity theft, Plaintiff Henry spent time and effort speaking on the phone with representatives from her bank, locking and replacing her compromised card, freezing her credit with Experian, and filing a complaint with both local police and the Federal Trade Commission. Also as a direct result of the breach, Plaintiff Henry spent time and money purchasing credit monitoring services from Experian in order to mitigate possible harm. Given the highly-sensitive nature of the information stolen, Plaintiff Henry remains at a substantial and imminent risk of future harm.

55. Plaintiff James McGonnigal is a resident and citizen of the State of Maryland, and his Personal Information was compromised in the Equifax data breach. Plaintiff McGonnigal verified through Equifax's data breach response website that his Personal Information was compromised. As a result of the breach, Plaintiff McGonnigal has suffered identity theft in the form of more than ten unauthorized retail credit cards opened or applied for in his name and using his Personal Information. As a result of this identity theft, Plaintiff McGonnigal spent time and effort completing affidavits for and placing fraud alerts with the banks

managing his retail credit accounts, contacting representatives from TransUnion's zendough credit monitoring, and cancelling and replacing his cards. Plaintiff McGonnigal also paid to maintain his credit monitoring services from zendough and placed credit freezes with Equifax, Experian, and TransUnion in order to mitigate possible harm. In addition, as a result of the breach, Plaintiff McGonnigal spent time and effort monitoring his financial accounts and took time away from work to manage the fallout from his identity theft. Given the highly-sensitive nature of the information stolen, Plaintiff McGonnigal remains at a substantial and imminent risk of future harm.

MASSACHUSETTS

56. Plaintiff Emily Knowles is a resident and citizen of the State of Massachusetts, and her Personal Information was compromised in the Equifax data breach. Plaintiff Knowles verified through Equifax's data breach response website that her Personal Information was compromised. As a direct result of the breach, Plaintiff Knowles spent time and money purchasing credit freezes from Equifax, Experian, and TransUnion in order to mitigate possible harm. Given the highly-sensitive nature of the information stolen, Plaintiff Knowles remains at a substantial and imminent risk of future harm.

57. Plaintiff Dallas Perkins is a resident and citizen of the State of Massachusetts, and his Personal Information was compromised in the Equifax data breach. Plaintiff Perkins verified through Equifax's data breach response website that his Personal Information was compromised. As a result of the breach, Plaintiff Perkins has suffered identity theft in the form of an unauthorized account applied for in his name and using his Personal Information. As a result of this identity theft, Plaintiff Perkins spent time and effort investigating and disputing the fraudulent activity. Also as a direct result of the breach, Plaintiff Perkins spent time and money purchasing credit monitoring and identity theft protection services from LifeLock in order to mitigate possible harm. In addition, as a result of the breach, Plaintiff Perkins spent time and effort reviewing his financial accounts and credit card statements for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Perkins remains at a substantial and imminent risk of future harm.

MICHIGAN

58. Plaintiff Justin Bakko is a resident and citizen of the State of Michigan, and his Personal Information was compromised in the Equifax data breach. Plaintiff Bakko verified through Equifax's data breach response website that his Personal Information was compromised. As a direct result of the breach,

Plaintiff Bakko spent time and money purchasing a credit freeze from TransUnion in order to mitigate possible harm. In addition, as a result of the breach, Plaintiff Bakko spent time and effort monitoring his financial accounts and searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Bakko remains at a substantial and imminent risk of future harm.

59. Plaintiff Jack Cherney is a resident and citizen of the State of Michigan, and his Personal Information was compromised in the Equifax data breach. Plaintiff Cherney verified through Equifax's data breach response website that his Personal Information was compromised. As a direct result of the breach, Plaintiff Cherney spent time and effort placing a credit freeze with Experian in order to mitigate possible harm. Plaintiff Cherney subsequently paid to unfreeze and refreeze his credit with Experian. In addition, as a result of the breach, Plaintiff Cherney spent time and effort monitoring financial accounts and searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Cherney remains at a substantial and imminent risk of future harm.

MINNESOTA

60. Plaintiff Robert J. Etten is a resident and citizen of the State of Minnesota, and his Personal Information was compromised in the Equifax data breach. Plaintiff Etten verified through Equifax's data breach response website that

his Personal Information was compromised. Before the announcement of the breach, Plaintiff Etten purchased identity theft protection services from Equifax using his credit card. Plaintiff Etten did not receive the benefit of his purchase of identity theft protection from Equifax because Equifax's inadequate data security practices subjected Plaintiff Etten to the precise type of harm he was seeking to protect against. Equifax also violated its agreement with Plaintiff Etten to safeguard the privacy and security of his information. Plaintiff Etten would not have purchased this product had he known of Equifax's inadequate data security practices. As a result of the breach, Plaintiff Etten has suffered identity theft in the form of unauthorized attempts to change his wireless cell phone plan and open new services and accounts using his Personal Information. Plaintiff Etten also received notice directly from Equifax through the mail that his credit card used to purchase Equifax products was compromised in the breach. As a result of the breach, Plaintiff Etten experienced unauthorized charges on this same credit card. As a result of this fraud, Plaintiff Etten spent time and effort canceling his credit card and requesting a replacement card. In addition, as a result of the breach, Plaintiff Etten spent time and effort searching for fraudulent activity and contacting representatives to determine the validity of the TrustedID Premier credit monitoring offered by Equifax. Given the highly-sensitive nature of the

information stolen, Plaintiff Etten remains at a substantial and imminent risk of future harm.

61. Plaintiff Jennifer Ann Harris is a resident and citizen of the State of Minnesota, and her Personal Information was compromised in the Equifax data breach. Plaintiff Harris verified through Equifax's data breach response website that her Personal Information was compromised. As a direct result of the breach, Plaintiff Harris spent time and money purchasing credit freezes from Equifax, Experian, and TransUnion and identity theft protection from IdentityForce in order to mitigate possible harm. Plaintiff Harris subsequently paid to unfreeze her credit with Equifax, Experian, and TransUnion for one day in order to process a loan and then paid to have the credit freezes reinstated. In addition, as a result of the breach, Plaintiff Harris spent time and effort contacting Equifax about her concerns regarding the breach. Given the highly-sensitive nature of the information stolen, Plaintiff Harris remains at a substantial and imminent risk of future harm.

62. Plaintiff Alexander Hepburn is a resident and citizen of the State of Minnesota, and his Personal Information was compromised in the Equifax data breach. Plaintiff Hepburn verified through Equifax's data breach response website that his Personal Information was compromised. As a result of the breach, Plaintiff Hepburn has suffered identity theft in the form of unauthorized loans and accounts

applied for in his name and using his Personal Information. As a result of this identity theft, Plaintiff Hepburn spent time and effort searching for additional fraudulent activity, placing a credit freeze, resolving the unauthorized items on his credit report, and repairing his credit report. Also as a result of the fraudulent accounts on his credit report, Plaintiff Hepburn's credit score dropped approximately 60 to 80 points, which affected his ability to secure a mortgage for the house he was seeking to purchase. Before the announcement of the breach, Plaintiff Hepburn purchased identity theft protection from Equifax. Plaintiff Hepburn did not receive the benefit of his purchase because Equifax's inadequate data security practices subjected Plaintiff Hepburn to the precise type of harm that he was seeking to protect against. Equifax also violated its agreement with Plaintiff Hepburn to safeguard the privacy and security of his information. Plaintiff Hepburn would not have purchased this product had he had known of Equifax's inadequate data security practices. Given the highly-sensitive nature of the information stolen, Plaintiff Hepburn remains at a substantial and imminent risk of future harm.

MISSISSIPPI

63. Plaintiff Joseph Packwood is a resident and citizen of the State of Mississippi, and his Personal Information was compromised in the Equifax data

breach. Plaintiff Packwood verified through Equifax's data breach response website that his Personal Information was compromised. As a result of the breach, Plaintiff Packwood has suffered identity theft in the form of unauthorized access to his bank accounts that resulted in thousands of dollars being fraudulently withdrawn. As a result of this identity theft, Plaintiff Packwood spent time and effort researching the fraudulent withdrawals from his account and requesting that his bank investigate the fraudulent activity. Further, the bank has not reimbursed the amount of the fraudulent withdrawals. In addition, as a result of the breach, Plaintiff Packwood spent time and effort monitoring his financial accounts. Given the highly-sensitive nature of the information stolen, Plaintiff Packwood remains at a substantial and imminent risk of future harm.

64. Plaintiff Terry Goza is a resident and citizen of the State of Mississippi, and his Personal Information was compromised in the Equifax data breach. Plaintiff Goza verified through Equifax's data breach response website that his Personal Information was compromised. As a direct result of the breach, Plaintiff Goza spent time and money purchasing credit freezes from Equifax, Experian, and TransUnion in order to mitigate possible harm. Given the highly-sensitive nature of the information stolen, Plaintiff Goza remains at a substantial and imminent risk of future harm.

MISSOURI

65. Plaintiff Kayla Ferrel is a resident and citizen of the State of Missouri, and her Personal Information was compromised in the Equifax data breach. Plaintiff Ferrel verified through Equifax's data breach response website that her Personal Information was compromised. As a result of the breach, Plaintiff Ferrel spent time and effort monitoring her credit and searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Ferrel remains at a substantial and imminent risk of future harm.

66. Plaintiff Tabitha Thomas Hawkins is a resident and citizen of the State of Missouri, and her Personal Information was compromised in the Equifax data breach. Plaintiff Hawkins verified through Equifax's data breach response website that her Personal Information was compromised. Before the announcement of the breach, Plaintiff Hawkins purchased credit monitoring services from Equifax. Plaintiff Hawkins did not receive the benefit of her purchase because Equifax's inadequate data security practices subjected Plaintiff Hawkins to the precise type of harm that she was seeking to protect against. Equifax also violated its agreement with Plaintiff Hawkins to safeguard the privacy and security of her information. Plaintiff Hawkins would not have purchased this product had she known of Equifax's inadequate data security practices. In addition, as a result of

the breach, Plaintiff Hawkins spent time and effort monitoring her accounts for fraudulent activity and making multiple telephone calls and visits to her financial institution. Given the highly-sensitive nature of the information stolen, Plaintiff Hawkins remains at a substantial and imminent risk of future harm.

MONTANA

67. Plaintiff Sabina Bologna is a resident and citizen of the State of Montana, and her Personal Information was compromised in the Equifax data breach. Plaintiff Bologna verified through Equifax's data breach response website that her Personal Information was compromised. As a result of the breach, Plaintiff Bologna has suffered identity theft in the form of an unauthorized credit card opened in her name and using her Personal Information. As a result of this identity theft, Plaintiff Bologna spent time and effort filing a police report, communicating with the credit card company that issued the fraudulent card, and communicating with a store where a fraudulent purchase was made. In addition, as a result of the breach, Plaintiff Bologna spent time and effort monitoring financial accounts and searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Bologna remains at a substantial and imminent risk of future harm.

68. Plaintiff Margaret M. Henkel is a resident and citizen of the State of Montana, and her Personal Information was compromised in the Equifax data breach. Plaintiff Henkel verified through Equifax's data breach response website that her Personal Information was compromised. As a direct result of the breach, Plaintiff Henkel paid to maintain her credit monitoring from Identity Guard in order to mitigate possible harm. In addition, as a result of the breach, Plaintiff Henkel spent time and effort searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Henkel remains at a substantial and imminent risk of future harm.

NEBRASKA

69. Plaintiff Aloha Kier is a resident and citizen of the State of Nebraska, and her Personal Information was compromised in the Equifax data breach. Plaintiff Kier verified through Equifax's data breach response website that her Personal Information was compromised. As a result of the breach, Plaintiff Kier has suffered identity theft in the form of an unauthorized credit card applied for in her name and using her Personal Information. As a result of this identity theft, Plaintiff Kier spent time and effort contacting her bank, monitoring her accounts, and changing the passwords associated with her account. Given the highly-

sensitive nature of the information stolen, Plaintiff Kier remains at a substantial and imminent risk of future harm.

NEVADA

70. Plaintiff Maria Schifano is a resident and citizen of the State of Nevada, and her Personal Information was compromised in the Equifax data breach. Plaintiff Schifano verified through Equifax's data breach response website that her Personal Information was compromised. As a direct result of the breach, Plaintiff Schifano spent time and money purchasing LifeLock Advantage credit monitoring and identity theft protection from LifeLock in order to mitigate possible harm. Before the announcement of the breach, Plaintiff Schifano purchased Equifax Complete Premier credit monitoring from Equifax. Plaintiff Schifano did not receive the benefit of her purchase because Equifax's inadequate data security practices subjected Plaintiff Schifano to the precise type of harm that she was seeking to protect against. Equifax also violated its agreement with Plaintiff Schifano to safeguard the privacy and security of her information. Plaintiff Schifano would not have purchased this product had she known of Equifax's inadequate data security practices. In addition, as a result of the breach, Plaintiff Schifano spent time and effort monitoring numerous bank and credit card

accounts. Given the highly-sensitive nature of the information stolen, Plaintiff Schifano remains at a substantial and imminent risk of future harm.

71. Plaintiff Clara Parrow is a resident and citizen of the State of Nevada, and her Personal Information was compromised in the Equifax data breach. Plaintiff Parrow verified through Equifax's data breach response website that her Personal Information was compromised. As a result of the breach, Plaintiff Parrow has suffered identity theft in the form of an unauthorized insurance claim applied for in her name and using her Personal Information. As a result of this identity theft, Plaintiff Parrow spent time and effort resolving the claim with her service provider. Given the highly-sensitive nature of the information stolen, Plaintiff Parrow remains at a substantial and imminent risk of future harm.

NEW HAMPSHIRE

72. Plaintiff Todd Heath is a resident and citizen of the State of New Hampshire, and his Personal Information was compromised in the Equifax data breach. Plaintiff Heath verified through Equifax's data breach response website that his Personal Information was compromised. As a direct result of the breach, Plaintiff Heath spent time and money purchasing credit freezes from Equifax, Experian, and TransUnion in order to mitigate possible harm. Plaintiff Heath subsequently paid to unfreeze his credit with TransUnion. In addition, as a result of

the breach, Plaintiff Heath spent time and effort monitoring his financial accounts and monitoring his credit by paying for and reviewing his credit reports. Given the highly-sensitive nature of the information stolen, Plaintiff Heath remains at a substantial and imminent risk of future harm.

NEW JERSEY

73. Plaintiff Christopher P. Dunleavy is a resident and citizen of the State of New Jersey, and his Personal Information was compromised in the Equifax data breach. Plaintiff Dunleavy verified through Equifax's data breach response website that his Personal Information was compromised. Before the announcement of the breach, Plaintiff Dunleavy purchased the Equifax Premier Plan and the Complete Family Plan identity theft protection and credit monitoring services from Equifax. Plaintiff Dunleavy did not receive the benefit of his purchase because Equifax's inadequate data security practices subjected Plaintiff Dunleavy to the precise type of harm that he was seeking to protect against. Equifax also violated its agreement with Plaintiff Dunleavy to safeguard the privacy and security of his information. Plaintiff Dunleavy would not have purchased these products had he known of Equifax's inadequate data security practices. In addition, as a result of the breach, Plaintiff Dunleavy spent time and effort monitoring financial accounts. Given the

highly-sensitive nature of the information stolen, Plaintiff Dunleavy remains at a substantial and imminent risk of future harm.

74. Plaintiff Michael Getz is a resident and citizen of the State of New Jersey, and his Personal Information was compromised in the Equifax data breach. Plaintiff Getz verified through Equifax's data breach response website that his Personal Information was compromised. Before the announcement of the breach, Plaintiff Getz purchased Equifax ID Patrol credit monitoring and identity theft protection services from Equifax. Plaintiff Getz did not receive the benefit of his purchase because Equifax's inadequate data security practices subjected Plaintiff Getz to the precise type of harm that he was seeking to protect against. Equifax also violated its agreement with Plaintiff Getz to safeguard the privacy and security of his information. Plaintiff Getz would not have purchased this product had he known of Equifax's inadequate data security practices. Given the highly-sensitive nature of the information stolen, Plaintiff Getz remains at a substantial and imminent risk of future harm.

NEW MEXICO

75. Plaintiff Dean Edward Armstrong is a resident and citizen of the State of New Mexico, and his Personal Information was compromised in the Equifax data breach. Plaintiff Armstrong verified through Equifax's data breach response

website that his Personal Information was compromised. As a result of the breach, Plaintiff Armstrong has suffered identity theft in the form of an unauthorized credit card account opened in his name and using his Personal Information. As a result of this identity theft, Plaintiff Armstrong spent time and effort speaking with representatives from the credit card company and LifeLock to terminate the fraudulent account and initiate a fraud investigation. Plaintiff Armstrong also paid to maintain his identity protection services from LifeLock in order to mitigate possible harm. Given the highly-sensitive nature of the information stolen, Plaintiff Armstrong remains at a substantial and imminent risk of future harm.

NEW YORK

76. Plaintiff Thomas Patrick Schneider is a resident and citizen of the State of New York, and his Personal Information was compromised in the Equifax data breach. Plaintiff Schneider verified through Equifax's data breach response website that his Personal Information was compromised. As a result of the breach, Plaintiff Schneider has suffered identity theft and fraud in the form of an unauthorized tax return filed in his name and using his Personal Information. As a result of this identity theft and fraud, Plaintiff Schneider spent time and money working with his accountant to file a legitimate tax return with the IRS, speaking with three different Equifax representatives for more than an hour, and searching

his credit accounts for additional fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Schneider remains at a substantial and imminent risk of future harm.

77. Plaintiff Gerry Tobias is a resident and citizen of the State of New York, and his Personal Information was compromised in the Equifax data breach. Plaintiff Tobias verified through Equifax's data breach response website that his Personal Information was compromised. As a result of the breach, Plaintiff Tobias has suffered identity theft in the form of three illegitimate accounts opened in his name and using his Personal Information, including with two financial institutions and a credit card company. As a result of this identity theft, Plaintiff Tobias spent time and effort traveling to his bank, filing a police report regarding the fraudulent activity, contacting Equifax and bank representatives by phone, and placing a freeze on his credit. Given the highly-sensitive nature of the information stolen, Plaintiff Tobias remains at a substantial and imminent risk of future harm.

78. Plaintiff Josh Grossberg is a resident and citizen of the State of New York, and his Personal Information was compromised in the Equifax data breach. Plaintiff Grossberg verified through Equifax's data breach response website that his Personal Information was compromised. As a result of the breach, Plaintiff Grossberg has suffered identity theft in the form of an unauthorized wireless phone

provider account opened in his name and using his Personal Information. As a result of this identity theft, Plaintiff Grossberg spent time and effort disputing the account and related charges, and monitoring his financial accounts for additional fraudulent activity. Also as a direct result of the breach, Plaintiff Grossberg spent time and money purchasing identity theft protection services from LifeLock in order to mitigate possible harm. Given the highly-sensitive nature of the information stolen, Plaintiff Grossberg remains at a substantial and imminent risk of future harm.

NORTH CAROLINA

79. Plaintiff James Gay is a resident and citizen of the State of North Carolina, and his Personal Information was compromised in the Equifax data breach. Plaintiff Gay verified through Equifax's data breach response website that his Personal Information was compromised. As a result of the breach, Plaintiff Gay has suffered identity theft in the form of unauthorized credit inquiries made using his name and Personal Information, unauthorized charges through his checking account, and an unauthorized bank account opened in his name and using his Personal Information. As a result of this identity theft, Plaintiff Gay spent time and effort calling and making multiple trips to his bank to resolve the identity theft issues, calling the companies with which the unauthorized credit inquiries were

placed to try to obtain information about the identity theft, and pulling credit reports to monitor his credit score. In addition, as a result of the breach, Plaintiff Gay spent time and effort contacting Equifax, TransUnion, and Experian to place freezes on his credit. Given the highly-sensitive nature of the information stolen, Plaintiff Gay remains at a substantial and imminent risk of future harm.

NORTH DAKOTA

80. Plaintiff Thomas Edward Crowell is a resident and citizen of the State of North Dakota, and his Personal Information was compromised in the Equifax data breach. Plaintiff Crowell verified through Equifax's data breach response website that his Personal Information was compromised. In addition, Plaintiff Crowell received notice directly from Equifax through the mail that his credit card previously used to purchase a credit freeze from Equifax was compromised in the breach. As a result of the breach, Plaintiff Crowell spent time and effort determining which of his credit cards was compromised and ensuring the proper card was cancelled. In addition, as a result of the breach, Plaintiff Crowell spent time and effort monitoring all of his financial accounts and searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Crowell remains at a substantial and imminent risk of future harm.

OHIO

81. Plaintiff David L. Kacur is a resident and citizen of the State of Ohio, and his Personal Information was compromised in the Equifax data breach. Plaintiff Kacur verified through Equifax's data breach response website that his Personal Information was compromised. As a direct result of the breach, Plaintiff Kacur spent time and money purchasing a credit freeze from Equifax in order to mitigate possible harm. In addition, as a result of the breach, Plaintiff Kacur spent additional time, money, and effort monitoring financial accounts, searching for fraudulent activity, and sending certified letters to Equifax in efforts to determine who had access to his information. Given the highly-sensitive nature of the information stolen, Plaintiff Kacur remains at a substantial and imminent risk of future harm.

OKLAHOMA

82. Plaintiff Richard Dale Parks is a resident and citizen of the State of Oklahoma, and his Personal Information was compromised in the Equifax data breach. Plaintiff Parks verified through Equifax's data breach response website that his Personal Information was compromised. As a direct result of the breach, Plaintiff Parks spent time and money purchasing identity theft protection services from LifeLock in order to mitigate possible harm. In addition, as a result of the

breach, Plaintiff Parks spent time and effort monitoring financial accounts and searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Parks remains at a substantial and imminent risk of future harm.

OREGON

83. Plaintiff Donald Angelechio is a resident and citizen of the State of Oregon, and his Personal Information was compromised in the Equifax data breach. Plaintiff Angelechio verified through Equifax's data breach response website that his Personal Information was compromised. As a result of the breach, Plaintiff Angelechio has suffered identity theft in the form of an unauthorized credit card and bank loan applied for in his name and using his Personal Information. As a result of this identity theft, Plaintiff Angelechio spent time and effort with the financial institution investigating and disputing the unauthorized credit card and bank loan. In addition, as a result of the breach, Plaintiff has spent time and effort monitoring his accounts and reviewing his credit. Given the highly-sensitive nature of the information stolen, Plaintiff Angelechio remains at a substantial and imminent risk of future harm.

84. Plaintiff Natasha Carr is a resident and citizen of the State of Oregon, and her Personal Information was compromised in the Equifax data breach.

Plaintiff Carr verified through Equifax's data breach response website that her Personal Information was compromised. As a result of the breach, Plaintiff Carr has suffered identity theft in the form of an unauthorized bank account and unauthorized credit card opened in her name and using her Personal Information. As a result of this identity theft, Plaintiff Carr spent time and effort with the financial institutions investigating and disputing the unauthorized bank account and credit card opened in her name and filing a police report regarding the fraudulent activity. Also as a direct result of the breach, Plaintiff Carr spent time and money purchasing credit monitoring and a credit freeze from TransUnion and Experian in order to mitigate possible harm. Given the highly-sensitive nature of the information stolen, Plaintiff Carr remains at a substantial and imminent risk of future harm.

PENNSYLVANIA

85. Plaintiff Anthony Mirarchi is a resident and citizen of the State of Pennsylvania, and his Personal Information was compromised in the Equifax data breach. Plaintiff Mirarchi verified through Equifax's data breach response website that his Personal Information was compromised. Before the announcement of the breach, Plaintiff Mirarchi purchased Equifax Complete and Complete Premier credit monitoring services from Equifax. Plaintiff Mirarchi did not receive the

benefit of his purchase because Equifax's inadequate data security practices subjected Plaintiff Mirarchi to the precise type of harm that he was seeking to protect against. Equifax also violated its agreement with Plaintiff Mirarchi to safeguard the privacy and security of his information. Plaintiff Mirarchi would not have purchased these products had he known of Equifax's inadequate data security practices. In addition, as a result of the breach, Plaintiff Mirarchi spent time and effort monitoring his financial accounts and searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Mirarchi remains at a substantial and imminent risk of future harm.

86. Plaintiff Joanne Klotzbaugh is a resident and citizen of the State of Pennsylvania, and her Personal Information was compromised in the Equifax data breach. Plaintiff Klotzbaugh verified through Equifax's data breach response website that her Personal Information was compromised. As a result of the breach, Plaintiff Klotzbaugh has suffered identity theft in the form of unauthorized loans, credit accounts, and credit cards opened and applied for in her name and using her Personal Information. As a result of this identity theft, Plaintiff Klotzbaugh spent time and money filing police reports, contacting fraud departments and creditors, disputing information in her credit file, and setting up fraud alerts. Also as a result of the fraudulent accounts on her credit report, Plaintiff Klotzbaugh's credit score

dropped, which affected her in that she was unable to open a new credit account. In addition, as a result of the breach, Plaintiff Klotzbaugh spent time and effort monitoring her financial accounts and searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Klotzbaugh remains at a substantial and imminent risk of future harm.

87. Plaintiff Leah Lipner is a resident and citizen of the State of Pennsylvania, and her Personal Information was compromised in the Equifax data breach. Plaintiff Lipner verified through Equifax's data breach response website that her Personal Information was compromised. As a direct result of the breach, Plaintiff Lipner spent time and money purchasing credit monitoring and identity theft protection from Identity Guard in order to mitigate possible harm. In addition, as a result of the breach, Plaintiff Lipner spent time and effort monitoring her financial accounts and searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Lipner remains at a substantial and imminent risk of future harm.

88. Plaintiff Christy Adams is a resident and citizen of the State of Pennsylvania, and her Personal Information was compromised in the Equifax data breach. Plaintiff Adams verified through Equifax's data breach response website that her Personal Information was compromised. Before the announcement of the

breach, Plaintiff Adams purchased Equifax Complete Advantage credit monitoring services from Equifax. Plaintiff Adams did not receive the benefit of her purchase because Equifax's inadequate data security practices subjected Plaintiff Adams to the precise type of harm that she was seeking to protect against. Equifax also violated its agreement with Plaintiff Adams to safeguard the privacy and security of her information. Plaintiff Adams would not have purchased this product had she known of Equifax's inadequate data security practices. In addition, as a result of the breach, Plaintiff Adams spent time and effort monitoring her financial accounts and searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Adams remains at a substantial and imminent risk of future harm.

RHODE ISLAND

89. Plaintiff Stephen Plante is a resident and citizen of the State of Rhode Island, and his Personal Information was compromised in the Equifax data breach. Plaintiff Plante verified through Equifax's data breach response website that his Personal Information was compromised. As a result of the breach, Plaintiff Plante has suffered identity theft in the form of an unauthorized account applied for in his name and using his Personal Information. Given the highly-sensitive nature of the

information stolen, Plaintiff Plante remains at a substantial and imminent risk of future harm.

90. Plaintiff John J. Pagliarulo is a resident and citizen of the State of Rhode Island, and his Personal Information was compromised in the Equifax data breach. Plaintiff Pagliarulo verified through Equifax's data breach response website that his Personal Information was compromised. As a result of the breach, Plaintiff Pagliarulo spent time and effort reviewing his financial accounts and searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Pagliarulo remains at a substantial and imminent risk of future harm.

SOUTH CAROLINA

91. Plaintiff Michael Louis Hornblas is a resident and citizen of the State of South Carolina, and his Personal Information was compromised in the Equifax data breach. Plaintiff Hornblas verified through Equifax's data breach response website that his Personal Information was compromised. As a result of the breach, Plaintiff Hornblas has suffered identity theft in the form of unauthorized accounts opened in his name and using his Personal Information. As a result of this identity theft, Plaintiff Hornblas spent time and effort filing a police report and working with remediation specialists provided by his credit union to address the damage

caused by the identity theft. Before the announcement of the breach, Plaintiff Hornblas purchased Equifax ID Patrol Premier credit monitoring services from Equifax. Plaintiff Hornblas did not receive the benefit of his purchase because Equifax's inadequate data security practices subjected Plaintiff Hornblas to the precise type of harm that he was seeking to protect against. Equifax also violated its agreement with Plaintiff Hornblas to safeguard the privacy and security of his information. Plaintiff Hornblas would not have purchased this product had he known of Equifax's inadequate data security practices. Given the highly-sensitive nature of the information stolen, Plaintiff Hornblas remains at a substantial and imminent risk of future harm.

92. Plaintiff Gregory Jacobs is a resident and citizen of the State of South Carolina, and his Personal Information was compromised in the Equifax data breach. Plaintiff Jacobs verified through Equifax's data breach response website that his Personal Information was compromised. As a result of the breach, Plaintiff Jacobs has suffered identity theft in the form of an unauthorized attempt to re-route his disability payments to an unknown bank account and address and unauthorized attempts to open cellular phone accounts with multiple wireless phone providers in his name and using his Personal Information. As a result of this identity theft, Plaintiff Jacobs spent time and effort traveling to the police station and filing a

police report. In addition, as a result of the breach, Plaintiff Jacobs spent time and effort monitoring his financial accounts for additional fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Jacobs remains at a substantial and imminent risk of future harm.

SOUTH DAKOTA

93. Plaintiff Pete Swiftbird is a resident and citizen of the State of South Dakota, and his Personal Information was compromised in the Equifax data breach. Plaintiff Swiftbird verified through Equifax's data breach response website that his Personal Information was compromised. As a direct result of the breach, Plaintiff Swiftbird paid to maintain his credit monitoring products from Geico in order to mitigate possible harm. In addition, as a result of the breach, Plaintiff Swiftbird spent time and effort searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Swiftbird remains at a substantial and imminent risk of future harm.

TENNESSEE

94. Plaintiff Jonathan Strausser is a resident and citizen of the State of Tennessee, and his Personal Information was compromised in the Equifax data breach. Plaintiff Strausser verified through Equifax's data breach response website that his Personal Information was compromised. As a result of the breach, Plaintiff

Strausser has suffered identity theft in the form of unauthorized activity and fraudulent purchases on his wireless phone account. As a result of this identity theft, Plaintiff Strausser spent time and effort contacting his wireless carrier's customer support, verifying his identity, and disputing the fraudulent purchases. In addition, as a result of the breach, Plaintiff Strausser spent time and effort monitoring his wireless and financial accounts and searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Strausser remains at a substantial and imminent risk of future harm.

TEXAS

95. Plaintiff Delitha J. May is a resident and citizen of the State of Texas and her Personal Information was compromised in the Equifax data breach. Plaintiff May verified through Equifax's data breach response website that her Personal Information was compromised. As a result of the breach, Plaintiff May has suffered identity theft in the form of unauthorized credit accounts opened in her name and using her Personal Information through a retail store and online payment company, and an attempt to open an unauthorized credit account in her name and using her Personal Information through an electronics retail store. As a result of this identity theft, Plaintiff May spent time and money opening a U.S. Post Office box, filing two police reports, and contacting the companies where the

fraudulent accounts were opened or attempted to be opened in her name. Also as a direct result of the breach, Plaintiff May spent time and money purchasing credit freezes from TransUnion and Experian. Given the highly-sensitive nature of the information stolen, Plaintiff May remains at a substantial and imminent risk of future harm.

96. Plaintiff Ricardo A. Clemente is a resident and citizen of the State of Texas, and his Personal Information was compromised in the Equifax data breach. Plaintiff Clemente verified through Equifax's data breach response website that his Personal Information was compromised. As a result of the breach, Plaintiff Clemente has suffered identity theft in the form of multiple unauthorized hard inquiries on his credit report. Before the announcement of the breach, Plaintiff Clemente purchased Equifax Complete Premier identity theft protection from Equifax. Plaintiff Clemente did not receive the benefit of his purchase because Equifax's inadequate data security practices subjected Plaintiff Clemente to the precise type of harm that he was seeking to protect against. Equifax also violated its agreement with Plaintiff Clemente to safeguard the privacy and security of his information. Plaintiff Clemente would not have purchased this product had he known of Equifax's inadequate data security practices. In addition, as a result of the breach, Plaintiff Clemente spent time and effort monitoring his financial

accounts, searching for fraudulent activity, and speaking to Equifax about the breach. Plaintiff Clemente attempted to sign up for free TrustedID Premier after learning of the breach, but was unable to, despite spending approximately 4 hours on the phone with Equifax regarding this issue. Given the highly-sensitive nature of the information stolen, Plaintiff Clemente remains at a substantial and imminent risk of future harm.

97. Plaintiff John R. Hammond is a resident and citizen of the State of Texas and his Personal Information was compromised in the Equifax data breach. Plaintiff Hammond verified through Equifax's data breach response website that his Personal Information was compromised. As a direct result of the breach, Plaintiff Hammond spent time and money purchasing credit freezes from TransUnion and Experian and credit monitoring from Identity Force. In addition, as a result of the breach, Plaintiff Hammond spent time and effort monitoring his and his wife's accounts for fraudulent activity and communicating with the Social Security Administration concerning complications arising from the breach. Given the highly-sensitive nature of the information stolen, Plaintiff Hammond remains at a substantial and imminent risk of future harm.

UTAH

98. Plaintiff Anna Solorio is a current resident and citizen of the State of Nebraska and previously resided in the State of Utah during the time period when the breach occurred and was announced by Equifax. Plaintiff Solorio's Personal Information was compromised in the Equifax data breach. Plaintiff Solorio verified through Equifax's data breach response website that her Personal Information was compromised. As a result of the breach, Plaintiff Solorio spent time and effort monitoring her financial accounts and signing up for TrustID Premier credit monitoring services from Equifax. Given the highly-sensitive nature of the information stolen, Plaintiff Solorio remains at a substantial and imminent risk of future harm.

99. Plaintiff Abby Lee Elliott is a current resident and citizen of the State of Kentucky and previously resided in the State of Utah during the time period when the breach occurred and was announced by Equifax. Plaintiff Elliott's Personal Information was compromised in the Equifax data breach. Plaintiff Elliott verified through Equifax's data breach response website that her Personal Information was compromised. As a direct result of the breach, Plaintiff Elliott spent time and money purchasing credit monitoring from AAA in order to mitigate

possible harm. Given the highly-sensitive nature of the information stolen, Plaintiff Elliott remains at a substantial and imminent risk of future harm.

VERMONT

100. Plaintiff David Bielecki is a resident and citizen of the State of Vermont, and his Personal Information was compromised in the Equifax data breach. Plaintiff Bielecki verified through Equifax's data breach response website that his Personal Information was compromised. Given the highly-sensitive nature of the information stolen, Plaintiff Bielecki remains at a substantial and imminent risk of future harm.

VIRGINIA

101. Plaintiff Bridgette Craney is a resident and citizen of the State of Virginia, and her Personal Information was compromised in the Equifax data breach. Plaintiff Craney verified through Equifax's data breach response website that her Personal Information was compromised. As a result of the breach, Plaintiff Craney has suffered identity theft in the form of unauthorized credit cards opened and applied for in her name and using her Personal Information. As a result of this identity theft, Plaintiff Craney spent time and effort speaking with her financial institutions, disputing charges, reversing the unauthorized accounts opened in her name, and sorting through communications regarding the unauthorized accounts.

Also as a result of the fraudulent accounts on her credit report, Plaintiff Craney's credit score dropped approximately 40 points. In addition, as a result of the breach, Plaintiff Craney spent time and effort monitoring her financial accounts and searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Craney remains at a substantial and imminent risk of future harm.

WASHINGTON

102. Plaintiff Kismet Harvey is a resident and citizen of the State of Washington, and her Personal Information was compromised in the Equifax data breach. Plaintiff Harvey verified through Equifax's data breach response website that her Personal Information was compromised. As a result of the breach, Plaintiff Harvey has suffered identity theft in the form of unauthorized accounts opened in her name and using her Personal Information, unauthorized loans applied for and opened in her name and using her Personal Information, and creditors contacting her about loans she never opened and for which she never applied. As a result of this identity theft, Plaintiff Harvey took time off work in an effort to resolve her identity theft. During this time, she spent multiple hours per day making phone calls, traveling to meet with different creditors, and monitoring her financial accounts to search for fraudulent activity. Plaintiff Harvey also spent time and

effort filing a police report. Also as a direct result of the breach, Plaintiff Harvey spent time and money purchasing credit monitoring from Experian and Armor in order to mitigate possible harm. Given the highly-sensitive nature of the information stolen, Plaintiff Harvey remains at a substantial and imminent risk of future harm.

103. Plaintiff Katie Van Fleet is a resident and citizen of the State of Washington, and her Personal Information was compromised in the Equifax data breach. Plaintiff Van Fleet verified through Equifax's data breach response website that her Personal Information was compromised. As a result of the breach, Plaintiff Van Fleet has suffered identity theft in the form of unauthorized accounts and credit cards opened in her name and using her Personal Information. As a result of this identity theft, Plaintiff Van Fleet spent time and effort notifying every creditor and company of fraud, obtaining multiple credit reports, adding a fraud alert, filing a police report, filing an FTC report, freezing her credit, alerting Chex Systems, calling the IRS, attempting to change her social security number, and attempting to change her driver's license number. Also as a direct result of the breach, Plaintiff Van Fleet spent time and money placing credit freezes with Experian and TransUnion in order to mitigate possible harm. Given the highly-sensitive nature

of the information stolen, Plaintiff Van Fleet remains at a substantial and imminent risk of future harm.

104. Plaintiff Francine Campbell is a resident and citizen of the State of Washington, and her Personal Information was compromised in the Equifax data breach. Plaintiff Campbell verified through Equifax's data breach response website that her Personal Information was compromised. As a direct result of the breach, Plaintiff Campbell spent time and money purchasing credit monitoring services from LifeLock in order to mitigate possible harm. In addition, as a result of the breach, Plaintiff Campbell spent time and effort searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Campbell remains at a substantial and imminent risk of future harm.

WEST VIRGINIA

105. Plaintiff Debra Lee is a resident and citizen of the State of West Virginia, and her Personal Information was compromised in the Equifax data breach. Plaintiff Lee verified through Equifax's data breach response website that her Personal Information was compromised. As a direct result of the breach, Plaintiff Lee spent time and money purchasing a credit freeze from Experian in order to mitigate possible harm. In addition, as a result of the breach, Plaintiff Lee spent time and effort monitoring her financial accounts and searching for

fraudulent activity. On September 13, 2017, Plaintiff Lee purchased a consumer report from Equifax. This report failed to inform Plaintiff Lee of the breach or potential harm she would suffer as a consequence of the breach. Given the highly-sensitive nature of the information stolen, Plaintiff Lee remains at a substantial and imminent risk of future harm.

WISCONSIN

106. Plaintiff Kyle Olson is a resident and citizen of the State of Wisconsin, and his Personal Information was compromised in the Equifax data breach. Plaintiff Olson verified through Equifax's data breach response website that his Personal Information was compromised. As a direct result of the breach, Plaintiff Olson spent time and money purchasing credit freezes from Equifax, Experian, and TransUnion in order to mitigate possible harm. Plaintiff Olson subsequently paid to unfreeze his credit with all three credit reporting agencies. In addition, as a result of the breach, Plaintiff Olson spent time and effort monitoring his financial accounts, searching for fraudulent activity, and monitoring his credit score. Given the highly-sensitive nature of the information stolen, Plaintiff Olson remains at a substantial and imminent risk of future harm.

107. Plaintiff Robert Anderson is a resident and citizen of the State of Wisconsin, and his Personal Information was compromised in the Equifax data

breach. Plaintiff Anderson verified through Equifax's data breach response website that his Personal Information was compromised. As a direct result of the breach, Plaintiff Anderson spent time and money purchasing credit monitoring from City Financial in order to mitigate possible harm. In addition, as a result of the breach, Plaintiff Anderson spent time and effort searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Anderson remains at a substantial and imminent risk of future harm.

WYOMING

108. Plaintiff Mel C. Orchard III is a resident and citizen of the State of Wyoming, and his Personal Information was compromised in the Equifax data breach. Plaintiff Orchard verified through Equifax's data breach response website that his Personal Information was compromised. As a result of the breach, Plaintiff Orchard spent time and effort researching the Equifax breach and searching for fraudulent activity. Given the highly-sensitive nature of the information stolen, Plaintiff Orchard remains at a substantial and imminent risk of future harm.

DEFENDANTS AND THEIR RELEVANT CORPORATE STRUCTURE

109. Defendant Equifax Inc. is a Georgia corporation, with its principal place of business in Atlanta, Georgia. Equifax is subject to the jurisdiction of this Court and may be served with process through its registered agent, Shawn

Baldwin, 1550 Peachtree Street, N.W., Atlanta, Fulton County, Georgia. Equifax Inc. is the parent company of Defendants Equifax Information Services LLC and Equifax Consumer Services LLC.

110. Defendant Equifax Information Services LLC is a Georgia limited liability company, with its principal place of business in Atlanta, Georgia. Equifax Information Services LLC is subject to the jurisdiction of this Court and may be served with process through its registered agent, Shawn Baldwin, 1550 Peachtree Street, N.W., Atlanta, Fulton County, Georgia.

111. Defendant Equifax Consumer Services LLC is a Georgia limited liability company, with its principal place of business in Atlanta, Georgia. Equifax Consumer Services LLC is subject to the jurisdiction of this Court and may be served with process through its registered agent, Shawn Baldwin, 1550 Peachtree Street, N.W., Atlanta, Fulton County, Georgia.

112. Defendants operate together as an integrated consumer reporting agency ("CRA") to prepare and furnish consumer reports for credit and other purposes. All three Defendants are both "consumer reporting agencies" and "nationwide reporting agencies" as defined by the Fair Credit Reporting Act ("FCRA").

113. In prior litigation, Equifax Inc. has taken the position that it is not a "consumer reporting agency" governed by the FCRA. *See* 15 U.S.C. § 1681a(f) ("The term 'consumer reporting agency' means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports."). However, as one district judge aptly noted, Equifax Inc. takes this position only against *pro se* litigants or on unopposed summary judgment motions in an effort to evade liability under the FCRA. *See Jones v. Equifax, Inc.*, No. 3:14-cv-678, 2015 WL 5092514, at *4 n.11 (E.D. Va. Aug. 27, 2015).

114. Equifax Inc. is in fact a consumer reporting agency. For purposes of the FCRA, Equifax Inc. has held itself out repeatedly to the public as the operating entity of the "Equifax" CRA. The branding, labels, and disclosures on Defendants' consumer website are dominated by "Equifax, Inc." titling. For example, on its website, Equifax sells its "Equifax Credit Report and Score" to consumers starting at $15.95. The website is devoid of disclosures that ECS or EIS have any role in this or other transactions.

115. ECS is similarly a CRA because for monetary fees it regularly engages in part in the practice of assembling and maintaining consumer report information in its operational relationship with Equifax Inc. and EIS. Likewise, EIS holds itself out as a "consumer reporting agency" as defined by section 1681a(f) of the FCRA.

116. The FCRA, through a rule mandated at section 1681x, expressly prohibits "a consumer reporting agency from circumventing or evading treatment as a consumer reporting agency" by means of corporate reorganization or restructuring. Despite this, Equifax has attempted to use its corporate structure to evade liability under the FCRA. *See, e.g.*, *Channing v. Equifax, Inc.*, No. 5:11-cv-293-FL, 2013 WL 593942, at *2 (E.D.N.C. Feb. 15, 2013); *Greear v. Equifax, Inc.*, No. 13-11896, 2014 WL 1378777 (E.D. Mich. Apr. 8, 2014).

117. 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 FCRA restricted information with sibling entity ECS so both entities, and ultimately Equifax Inc., can market and profit from the sale of consumer identity theft protection products, including the blurring of legal lines

between providing file information under the FCRA versus for private sale to the consumer.

118. 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 and ECS as dependent and integrated divisions rather than as separate legal entities. 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 and ECS 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 breach itself, and Defendants' response to the breach.

119. 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 and ECS were merely alter egos of Equifax Inc. For purposes of how consumer data was handled, warehoused, used, and sold, the corporate distinctions were disregarded in practice. EIS and ECS were mere instrumentalities 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 subsidiaries no longer existed.

120. 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).

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

STATEMENT OF FACTS

The Importance of Consumer Credit in the U.S. Economy

122. A consumer credit system allows consumers to borrow money or incur debt, and to defer repayment of that money over time. Access to credit enables consumers to buy goods or assets without having to pay for them in cash at the time of purchase.[1] Nearly all Americans rely on credit to make everyday

[1] 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 11, 2018) ("FTC, *Consumer Credit Law & Practice in the U.S.*").

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.

123. In order for this system of credit to be efficient and effective, a system of evaluating the credit of consumers is required. The earliest American systems of credit evaluation were retailers relying on personal reputation and standing in the community to determine creditworthiness. U.S. credit reporting agencies started as associations of retailers who shared their customers' credit information with each other including those deemed as credit risks.[2]

124. As the nation grew after World War II, and banks and finance companies took over from retailers as the primary source of consumer credit, a more quantitative and objective system of credit rating emerged. The development of computers, which could store and process large amounts of data, enabled the CRAs to efficiently collect and provide credit information to consumer lenders on a national basis.[3]

125. Today, creditors such as banks and mortgage companies 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 all of the payment history

[2] *Id.*
[3] *Id.* at 2.

they receive relating to a single consumer and compile that information as part of a consumer's credit reporting "file."[4]

126. A consumer's credit reporting file contains identifying information such as the consumer's name, date of birth, address, and Social Security Number (SSN), 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 that loan. A consumer file also contains details on the consumer's payment history on past credit accounts—which helps potential lenders estimate how likely the consumer is to pay back the full amount of a loan on time—and information in the public record which might affect the consumer's ability to pay back a loan, such as recent bankruptcy filings, pending lawsuits, or information relating to tax liabilities.[5]

127. Because consumers have little or no control over the information that CRAs gather and store, the accuracy and security of the information they compile is at the heart of a fair and accurate credit reporting system. Information that is inaccurate can lead to uninformed credit decisions, and information that is

[4] *Id.*

[5] *Id.* at 1.

unsecure can lead to identify theft, fraud, and widespread distrust of CRAs—with systemic consequences for the entire national economy.

Equifax Compiles Massive Amounts of Consumer Information

128. Equifax first did business in 1899 as Retail Credit Company. At that time, most of its operation was dedicated to gathering information for insurance companies, including information on people's finances, health, moral beliefs, vehicle use and other factors that insurance companies used when quoting for life, car, and health insurance policies. Critics asserted that Retail Credit Company "reinforced preexisting social inequalities and rationalized 'fair' discrimination as a cornerstone of the capitalist economy. For women and poor African Americans, for example, a Retail Credit Company report did not open doors to financial security. It just recorded how society already saw you: as a bad risk."[6]

129. By the mid-1960s, Retail Credit Company had nearly 300 branch offices and maintained files on millions of Americans. The company sold stock to the public for the first time in 1965. While many CRAs at the time gathered only names, birth dates, address, and payment history for consumers, "Retail Credit

[6] Rachel Bunker, *The Equifax Way*, JACOBIN MAGAZINE (Sept. 18, 2017), https://www.jacobinmag.com/2017/09/equifax-retail-credit-company-discrimination-loans (last accessed May 11, 2018).

Company, which specialized in insurance reporting, gathered far more information on consumers."[7]

130. An article published in the New Republic in 1966 documented how Retail Credit Company "inspectors" and investigators "collected the most intimate details of an individual's life, including information about their race and sexual habits, their church attendance, their home environment, and whether or not they were experiencing marital discord."[8] The article warned that the information "could have originated from potentially unreliable neighbors and acquaintances" and that "[i]f damaging or just plain wrong information had managed to creep into a person's file, they were at the mercy of the credit bureau, since it was nearly impossible to see these confidential consumer reports."[9]

131. In March 1970, Alan Westin, a Columbia University professor, wrote an article critical of Retail Credit Company in *The New York Times* after reviewing a sample of the company's files and discovering that they included "facts, statistics, inaccuracies, and rumors" about virtually every phase of an individual's life, including "marital troubles, jobs, school history, childhood, sex life and political activities."

[7] *Id.*

[8] *Id.*

[9] *Id.*

132. That same month, as Retail Credit Company moved towards digitizing its records, Westin testified before Congress about how widespread inaccuracies could result in consumers being unfairly denied credit. In response, Congress enacted the enacted the FCRA in October 1970 "to promote the accuracy, fairness, and privacy of consumer information contained in the files of consumer reporting agencies."

133. To fend off negative publicity and help improve its image, in late 1975 Retail Credit Company changed its name to "Equifax Inc." Over the next two decades, Equifax expanded rapidly by acquiring many of its rivals and increasing its data collection capacity. By the late 1990s, industry consolidation resulted in three major CRAs controlling the market: Equifax, Experian, and TransUnion.

134. Equifax's business model involves aggregating data relating to consumers from various sources, compiling that data in a usable format known as a credit report, and selling access to those reports to lenders interested in making credit decisions, 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.[10]

135. Equifax also sells information directly to consumers, including access to their own credit file (known as a "consumer disclosure"). In 2001, Equifax partnered with the Fair Isaac Corporation ("FICO") to allow consumers to purchase their three-digit FICO credit scores, which are numerical values generated to represent the "creditworthiness" of a consumer. Equifax sells a number of credit-related products tailored to consumers and businesses interested in monitoring their credit. Today, Equifax's consumer business alone generates $400 million in annual sales.

136. In addition to providing services to individual consumers, Equifax supplies identity verification services to the U.S. Social Security Administration and works with the federal Centers for Medicare and Medicaid Services to verify eligibility for health-insurance subsidies. These services include helping consumers check their Social Security benefits and request replacement Social Security cards,

[10] AnnaMaria Androitis, Michael Rapoport, and 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 (last accessed May 11, 2018).

as well as to verify eligibility for subsidies to buy health insurance under the Affordable Care Act.

137. Equifax recognizes that the value of its company is inextricably tied to its massive trove of consumer data. For that reason, Equifax has aggressively acquired companies with the goal of expanding into new markets and acquiring proprietary data sources.[11]

138. For example, in 2002 Equifax acquired Naviant Inc. for $135 million and gained access to Naviant's database of more than 100 million permission-based e-mail addresses.

139. In 2007, Equifax expanded its database of payroll information by acquiring TALX Corporation for $1.4 billion, which at the time held employment records on 142 million individuals. Following this acquisition, Equifax began offering a service called "The Work Number" that was designed to provide automated employment and income verification for prospective employers and allow anyone whose employer uses the service to provide proof of their income

[11] *Id.*

when purchasing a home or applying for a loan.[12] Equifax ultimately persuaded more than 7,000 employers to hand over salary details for this income verification system that encompasses nearly half of American workers.[13]

140. In 2009, Equifax paid $124 million in cash for IXI Corporation, a company specializing in collecting, analyzing and delivering consumer wealth and asset data. In its 2009 Annual Report, Equifax stated that, "The data and intelligence we derive from our broad base of assets—200+ million U.S. credit files; 200+ million records at The Work Number; $10 trillion in consumer wealth data from IXI; the National Consumer Telecom & Utilities Exchange; and the 26 million files of small business information—are unique and not replicable."

141. In 2010, Equifax acquired Anakam, Inc., an authentication management vendor that offered products addressing online identify verification, credentialing, and two-factor authentication. This acquisition permitted Equifax to

[12] Brian Krebs, *Equifax Breach Fallout: Your Salary History*, KREBS ON SECURITY (Oct. 17, 2017), https://krebsonsecurity.com/2017/10/equifax-breach-fallout-your-salary-history/ (last accessed May 11, 2018) ("Krebs, *Equifax Breach Fallout: Your Salary History*").

[13] Stacy Cowley and Tara Siegel Bernard, *As Equifax Amassed Ever More Data, Safety Was a Sales Pitch*, THE NEW YORK TIMES (Sept. 23, 2017), https://www.nytimes.com/2017/09/23/business/equifax-data-breach.html?smprod=nytcore-ipad&smid=nytcore-ipad-share#story-continues-2 (last accessed May 11, 2018).

sell to businesses identity and authentication systems that utilized consumers' credit information in order to verify the consumer's identity.

142. In 2012, Equifax paid $1 billion to absorb the largest independent CRA in the U.S., Computer Science Corp., which held credit files in 15 U.S. states covering 20 percent of the country's population.

143. In 2014, Equifax acquired TDX Group, a UK-based debt-management firm, for $327 million in order to expand its debt-collection capabilities. In 2016, Equifax acquired Veda Group Limited, the leading provider of credit information and analysis in Australia and New Zealand, for $1.7 billion.

144. Equifax now maintains information on over 820 million individuals and 91 million businesses worldwide. It is publicly traded on the New York Stock Exchange (ticker symbol EFX), and generated revenues of $3.362 billion in 2017.

145. Equifax's strategy of rapid expansion by adding new data sources and increasing profits came with one major caveat: Equifax was unwilling to make corresponding investments in data security to protect the highly sensitive information it continued to accumulate. And this directive came straight from the top. As noted by *The New York Times* in a September 2017 article: "Equifax's

chief executive had a simple strategy when he joined more than a decade ago: Gather as much personal data as possible and find new ways to sell it."[14]

Equifax Recognized the Importance of Data Security

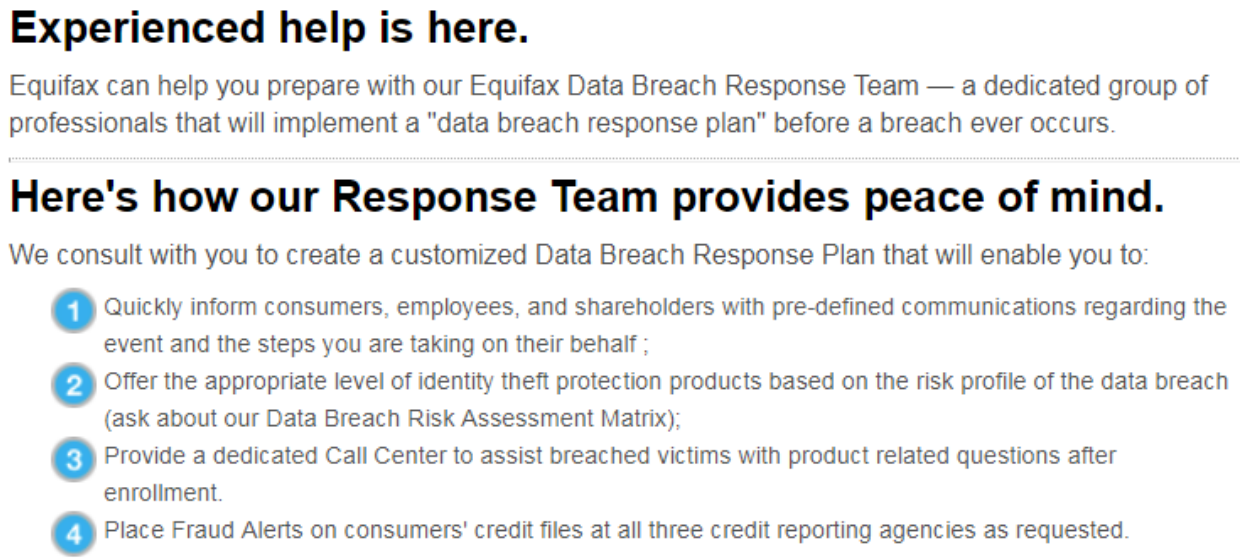
146. Equifax was well aware of the likelihood and repercussions of cybersecurity threats, including data breaches, having observed numerous other well-publicized data breaches involving major corporations over the last decade plus. In fact, Equifax sought to capitalize on the increase in the number of breaches by spending nearly $100 million since 2013 to acquire two identity theft protection and resolution companies—Trusted ID and ID Watchdog—to bolster its data breach response and product offerings.

147. As evidenced by its own product offerings, Equifax held itself out as a leader and expert in anticipating and combatting such threats and developed and sold "data breach solutions" to consumers and businesses to combat the "great risk of identity theft and fraud." Equifax even maintained a dedicated landing page to sell products and services specifically tailored to a data breach: www.equifax.com/help/data-breach-solutions.

[14] *Id.*

148. In its marketing materials, copied below, 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."

149. Equifax has also 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 breach, offering identity theft protection products, providing a dedicated call center to assist breach victims, and placing fraud alerts on consumers' credit files.



Experienced help is here.

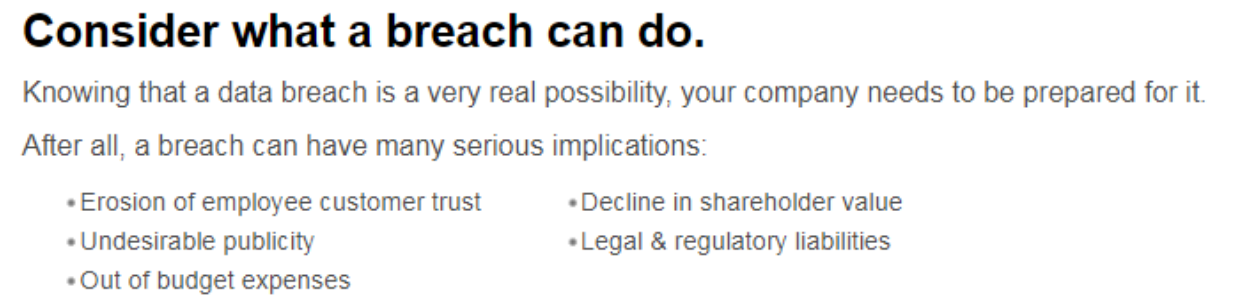
Equifax can help you prepare with our Equifax Data Breach Response Team — a dedicated group of professionals that will implement a "data breach response plan" before a breach ever occurs.

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.

150. 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.



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

151. Equifax also made representations to consumers regarding its data privacy practices. On its website, Equifax's summary statement of its Privacy Policy states: "For more than 100 years, Equifax has been a catalyst for commerce by bringing businesses and consumers together. Equifax also provides products and services that bring businesses together with other businesses. We have built

our reputation on our commitment to deliver reliable information to our customers (both businesses and consumers) and to protect the privacy and confidentiality of personal information about consumers. We also protect the sensitive information we have about businesses. Safeguarding the privacy and security of information, both online and offline, is a top priority for Equifax."[15]

Privacy

For more than 100 years, Equifax has been a catalyst for commerce by bringing businesses and consumers together. Equifax also provides products and services that bring businesses together with other businesses.

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

152. The full text of Equifax's Privacy Policy states, among other things, that Equifax "restrict[s] access to personally identifiable information . . . that is collected about you to only those who have a need to know that information in connection with the purpose for which it is collected and used."

153. Equifax agreed 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 agreed that "we have security protocols and measures in place to protect the personally identifiable

[15] http://www.equifax.com/privacy/ (last accessed May 11, 2018).

information . . . and other information we maintain 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."

154. Equifax's Privacy Policy further states: "We will not disclose your personal information to third parties except to provide you with the disclosure or service you request, or under certain circumstances as described in this policy."

155. In its Form 10-K from 2016, Equifax claimed that it was 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." The following year, Equifax included: "Data is at the core of our value proposition and the protection and safeguarding of that information is paramount."

156. Equifax also imposed stringent requirements on the businesses that purchase consumer information from Equifax, explicitly recognizing the parties' collective duty to protect consumer information. For example, in its form Broker Subscription Agreement, Equifax requires that:

a. "only Authorized Users can order or have access to" protected information;

b. credit reports are not provided "to any third party except as permitted";

c. protected information "must be encrypted when not in use and all printed [protected information] must be stored in a secure, locked container when not in use, and must be completely destroyed when no longer needed by cross-cut shredding machines (or other equally effective destruction method) such that the results are not readable or useable for any purpose";

d. protected information must be encrypted with: "Advanced Encryption Standard (AES), minimum 128-bit key or Triple Data Encryption Standard (3DES), minimum 168-bit key, encrypted algorithms";

e. Equifax's business partner must "monitor compliance" with these obligations "and immediately notify EQUIFAX if [the business partner] suspects or knows of any unauthorized access or attempt to access the" protected information;

f. Equifax's business partner must "not ship hardware or software . . . to third parties without deleting . . . any consumer information";

g. Equifax's business partner must "use commercially reasonable efforts to assure data security when disposing of any consumer report information";

h. "Such efforts must include the use of those procedures issued by [applicable agencies], "e.g. the Federal Trade Commission . . . ."

157. With regard to network security, Equifax acknowledges and requires that its business partners must "use commercially reasonable efforts to protect EQUIFAX Information when stored on servers", subject to the following requirements:

- "EQUIFAX Information must be protected by multiple layers of network security, including but not limited to, firewalls, routers, intrusion detection device";
- "secure access (both physical and network) to systems storing EQUIFAX Information must include authentication and passwords that are changed at least every 90 days";
- "all servers must be kept current and patched on a timely basis with appropriate security-specific system patches, as they are available."

158. In 2017, Equifax's Chief Information Security Officer ("CISO"), Susan Mauldin, gave an interview about "how the role of a Chief Information Security Officer has evolved in response to growing cybersecurity threats."[16] In the interview, Ms. Mauldin discussed at length her methods for addressing expected cybersecurity threats, stating that "[w]e 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."[17] 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.

[16] http://archive.is/6M8mg (last accessed May 11, 2018). Shortly after the breach, the active article was removed from the internet, and only an archive of the file remains.

[17] *Id*.

159. Equifax's awareness of the importance of data security was bolstered in part by its observation of numerous other well-publicized data breaches involving major corporations being targeted for consumer information in the years preceding the Equifax breach.

160. Through a series of data breaches extending back to 2013, more than three billion Yahoo user accounts were compromised when accountholders' names, addresses, and dates of birth were stolen. The hackers also stole users' passwords, both encrypted and unencrypted, and security questions and answers.

161. In separate incidents in 2013 and 2014, hundreds of millions of retail customers were victimized by hacks of payment card systems at Target Stores and The Home Depot. Both breaches led to rampant payment card fraud and other damages both to consumers and to the card-issuing banks.

162. In summer 2014, a data breach of JP Morgan Chase compromised the data of 76 million American households and 7 million small businesses. Breached data included contact information (names, addresses, phone numbers, and email addresses) as well as "internal information about the users."

163. In early 2015, Anthem, the second-largest health insurer in the United States, suffered a data breach that exposed the names, addresses, Social Security

numbers, dates of birth, and employment histories of nearly 80 million current and former plan members.

164. In September 2015, credit reporting agency Experian, Equifax's largest competitor, acknowledged that an unauthorized party accessed one of its servers containing the names, addresses, Social Security numbers, dates of birth, driver's license, military ID, and/or passport numbers, and additional information of more than 15 million consumers over a period of two years.

165. Dozens of other data breaches over the past few years were well known to information technology ("IT") and security professionals across the country, and particularly Equifax. 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 he referred to consumer fraud as a "huge opportunity" and "massive, growing business" for Equifax.[18]

[18] 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 (last accessed May 11, 2018) ("Puzzanghera, *Senators Slam Equifax*"); 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/ (last accessed May 11, 2018).

Equifax Has a History of Inadequate Data Security Practices

166. Given the amount of sensitive data it compiles and stores, Equifax was well aware it was a target, but nonetheless refused to implement best practices relating to data security—as demonstrated by the numerous data security lapses Equifax has experienced over the last 10 years.

167. In 2010, tax forms mailed by Equifax's payroll vendor had Equifax employees' SSNs partially or fully viewable through the envelope's return address window. One affected Equifax employee stated, "If they can't do this internally how are they going to be able to go to American Express and other companies and say we can mitigate your liability? . . . They are first-hand delivering information for the fraudsters out there. It's so terribly sad. It's just unacceptable, especially from a credit bureau."[19]

168. In March of 2013, all three major credit reporting agencies acknowledged intrusions into their systems after information pertaining to

[19] Elinor Mills, *Equifax tax forms expose worker Social Security numbers*, CNET (Feb. 11, 2010), http://www.cnet.com/news/equifax-tax-forms-expose-worker-social-security-numbers/ (last accessed May 11, 2018).

celebrities and high-profile figures ended up on the *Exposed* website.[20] Attackers gained fraudulent and unauthorized access to credit reports and other personal sensitive information for former First Lady Michelle Obama, Paris Hilton, former Secretary of State Hillary Clinton, and former FBI Director Robert Mueller.[21] In addition, hackers gained access to publicly available information on individuals to answer security questions, which enabled them to bypass the credit bureaus' authentication measures.[22] This breach was called a "juvenile hack" but proved that the credit reporting agencies struggled to "properly authenticat[e] users attempting to view their credit report."[23] Despite this incident, Equifax stated in its February 28, 2014 Annual Report that it "ha[d] not experienced any material breach of cybersecurity."

169. Starting in April 2013, an IP address operator was able to obtain credit reports using sufficient personal information to meet Equifax's identity verification process. On January 31, 2014, Equifax's security team discovered a suspicious

[20] David Bisson, *4 Credit Bureau Breaches that Predate the 2017 Equifax Hack*, TRIPWIRE (Sept. 14, 2017), https://www.tripwire.com/state-of-security/security-data-protection/4-credit-bureau-data-breaches-predate-2017-equifax-hack/ (last accessed May 11, 2018).

[21] Robert Westervelt, *Equifax, Other Credit Bureaus Acknowledge Data Breach*, CRN (Mar. 13, 2013), https://www.crn.com/news/security/240150683/equifax-other-credit-bureaus-acknowledge-data-breach.htm (last accessed May 11, 2018).

[22] *Id.*

[23] *Id.*

pattern of inquiries and blocked the IP address from further access. Equifax acknowledged that from April 2013 to January 31, 2014, the IP address operator may have made unauthorized and fraudulent requests for Equifax credit reports. Equifax reported the suspicious activity to the FBI and offered affected individuals a one-year subscription to its credit monitoring service.[24]

170. In 2014, Equifax left private encryption keys on its server, allowing anyone who accessed the server to obtain the keys and decrypt encrypted data into its original form.[25]

171. In 2015, Equifax exposed consumer data as a result of another "technical error," this time one that "occurred during a software change."[26] Also in March 2015, Equifax sent a Maine woman the full credit reports of more than 300 other individuals, which exposed their social security numbers, dates of birth, current and previous addresses, creditor information, and bank and loan account

[24] Letter from Equifax Legal Department to Attorney General Joseph Foster Regarding Security Breach Notification (Mar. 5, 2014) at 1, https://www.doj.nh.gov/consumer/security-breaches/documents/equifax-20140305.pdf (last accessed May 11, 2018) .

[25] Brian Krebs (@briankrebs), TWITTER (Sept. 15, 2017 8:59 AM), https://twitter.com/briankrebs/status/908722014449520642 (last accessed May 11, 2018).

[26] Letter from King & Spalding LLP to Attorney General Joseph Foster Regarding Data Incident Notification (Apr. 2, 2015) at 1, https://www.doj.nh.gov/consumer/security-breaches/documents/equifax-20150402.pdf (last accessed May 11, 2018).

numbers, among other sensitive information. The woman told reporters "I'm not supposed to have this information, this is unbelievable, someone has messed up."[27] In response, Equifax's Vice President of Corporate Communications, Tim Klein, said, "This is a high priority. Obviously, this is a serious situation. I'm going to get our security and forensics teams involved."

172. In 2016, a security researcher found a common vulnerability known as cross-site scripting (XSS) on the main Equifax website. XSS bugs allow attackers to send specially-crafted links to Equifax customers and, if the target clicks through and is logged into the site, their username and password can be revealed to the hacker. The researcher reported that the bug had not been fixed even months after it was initially made known to Equifax.[28]

173. In May 2016, it was discovered that a product offered by Equifax's subsidiary company Equifax Workforce Solutions, Inc. (d/b/a TALX), a purveyor of electronic W-2 forms accessible for download for many companies, contained a major security vulnerability that allowed data thieves "to access W-2 data merely

[27] Jon Chrisos, *Credit agency mistakenly sends 300 confidential reports to Maine woman*, BANGOR DAILY NEWS (March 19, 2015), http://bangordailynews.com/2015/03/19/news/state/credit-agency-mistakenly-sends-300-confidential-reports-to-maine-woman/ (last accessed May 11, 2018).

[28] 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/#671ed1c677c0 (last accessed May 11, 2018).

by entering at Equifax's portal the employee's default PIN code, which was nothing more than the last four digits of the employee's Social Security number and their four-digit birth year" including employees of grocery chain Kroger.[29] That same month, Stanford University identified approximately 600 employees whose W-2 data was hacked through Equifax's W-2 Express portal.[30] Again in April of 2016, Northwestern University notified approximately 150 employees whose salary and tax data was breached through Equifax.[31]

174. In August of 2016, in light of all of these previous breaches, institutional investor advisor MSCI, Inc. cautioned that Equifax was ill-prepared to face the "increasing frequency and sophistication of data breaches."[32] As a result,

[29] Brian Krebs, *Crooks Grab W-2s from Credit Bureau Equifax*, KREBS ON SECURITY (May 16, 2016), https://krebsonsecurity.com/2016/05/crooks-grab-w-2s-from-credit-bureau-equifax/ (last accessed May 11, 2018) ("Krebs, *Crooks Grab W-2s from Credit Bureau Equifax*").

[30] Hannah Knowles, *University employees vulnerable after tax data breach*, THE STANFORD DAILY (Apr. 12, 2016), https://www.stanforddaily.com/2016/04/12/university-employees-vulnerable-after-tax-data-breach/ (last accessed May 11, 2018); *see also* Krebs, *Crooks Grab W-2s from Credit Bureau Equifax*.

[31] See Krebs, *Crooks Grab W-2s from Credit Bureau Equifax*.

[32] Asjylyn Loder, *A Warning Shot on Equifax: Index Provider Flagged Security Issues Last Year*, THE WALL STREET JOURNAL (Oct. 6, 2017), https://www.wsj.com/articles/a-warning-shot-on-equifax-index-provider-flagged-security-issues-last-year-1507292590 (last accessed May 11, 2018).

MSCI downgraded Equifax to a "CCC" grade for its environmental, social and governance risks—the lowest rating used by the company.

175. Several months later, in December of 2016, just a few months before the breach at issue in this case, a security researcher warned Equifax that one of its 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."[33] The researcher was able to access full names, Social Security numbers, birth dates, and city and state of residence information for affected consumers. The flaw was discovered on a webpage that appeared to be a portal for employees. The webpage contained multiple search boxes and allowed anyone to force the site to display the personal information of Equifax customers and credentials that were needed to access the search page. The researcher was also able to take control of several Equifax servers and found that the servers were

[33] Lorenzo Franceschi-Bicchierai, *Equifax Was Warned*, VICE (Oct. 26, 2017), https://motherboard.vice.com/en_us/article/ne3bv7/equifax-breach-social-security-numbers-researcher-warning (last accessed May 11, 2018) ("Franceschi-Bicchierai, *Equifax Was Warned*").

running outdated software that was vulnerable to breach. It took the company six months to patch that vulnerability.[34]

176. The next month, in January of 2017, Equifax received a report that a member of credit monitoring service LifeLock was able to view another person's credit report. 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."[35]

177. Given the condition of Equifax's security and software management, multiple third parties concluded that, given the condition of its security and software management, Equifax was highly susceptible to a breach in 2017.

178. For example, four independent analyses of Equifax cybersecurity, conducted either before or immediately after the breach, identified important weaknesses including that Equifax "was behind on basic maintenance of websites

[34] George Cox, *Equifax suffers another security breach*, THE SPECTRUM (Nov. 8, 2017), https://www.thespectrum.com/story/life/features/mesquite/2017/11/08/equifax-suffers-another-security-breach/842717001/ (last accessed May 11, 2018).

[35] 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 (last accessed May 11, 2018).

that could have been involved in transmitting sensitive consumer information and scored poorly in areas" highly relevant to potential breaches.[36]

179. In April 2017—the month before the 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."[37]

180. 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."[38]

181. An outside review by 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

---

[36] AnnaMaria Androitis and Robert McMillan, *Equifax Security Showed Signs of Trouble Months Before Hack*, THE WALL STREET JOURNAL (Sept. 26, 2017), https://www.wsj.com/article_email/equifax-security-showed-signs-of-trouble-months-before-hack-1506437947-1MyQjAxMTA3OTIyNjUyMzY5Wj/ (last accessed May 11, 2018). *See also Bad Credit: Uncovering Equifax's Failure to Protect Americans' Personal Information* (Feb. 7, 2018), https://www.warren.senate.gov/files/documents/2018_2_7_%20Equifax_Report.pdf (last accessed May 11, 2018) ("Warren Report").

[37] *Id.*

[38] *Id.*

2017 when the breach had already occurred. The FICO analysis found that public-facing websites run by Equifax had expired certificates, and there were errors in the chain of certificates and other web-security issues. Certificates are used to validate the connection between a user's web browser and an HTTPS web server, allowing users to know that their connection to a website is legitimate and secure.

182. A fourth independent review released just after the breach was revealed identified significant problems with Equifax cybersecurity. This report by BitSight Technologies gave the company an "'F" in application security and a "D" for software patching.[39]

The Equifax Data Breach

183. Equifax maintains a consumer dispute website where consumers can go online to dispute inaccurate information contained on their credit reports. This website runs on Apache Struts software, which is a popular programming framework for building web applications in Java.

184. Apache Struts makes it "easier for developers to build top-to-bottom custom websites" and it "can handle everything from interactive screens and

[39] See Warren Report at 5.

logins, to web apps and database management."[40] 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.

185. 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,[41] its popularity and expansive capabilities leaves 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 underlying system and can "execute commands just like they were the administrators." In other words, "they basically control the system."[42]

186. On March 6, 2017, a serious vulnerability in the Apache software was discovered and reported. The discovery of this vulnerability was described as a

[40] Ben Popken, *Equifax Hackers Exploited Months-Old Flaw*, NBC NEWS (Sept. 14, 2017), https://www.nbcnews.com/business/consumer/how-did-equifax-hack-even-happen-n801331 (last accessed May 11, 2018) ("Popken, *Equifax Hackers Exploited Months-Old Flaw*").

[41] Keith Collins, *The hackers who broke into Equifax exploited a flaw in open-source server software*, QUARTZ (Sept. 8, 2017), https://qz.com/1073221/the-hackers-who-broke-into-equifax-exploited-a-nine-year-old-security-flaw/ (last revised Sept. 14, 2017) (last accessed May 11, 2018).

[42] See Popken, *Equifax Hackers Exploited Months-Old Flaw*.

"hair on fire moment" in the IT world that caused all affected IT professionals to scramble for a fix.[43]

187. On March 7, 2017, one day after the vulnerability in the Apache software was discovered, the Apache Software Foundation issued a "patch" to address the flaw, and warned its customers of the risk and the need to implement the patch.[44]

188. On March 8, 2017, Equifax received a specific and detailed warning from the Department of Homeland Security's U.S. Computer Emergency Readiness Team ("CERT") regarding the Apache Struts vulnerability and available patch.[45]

189. On March 9, 2017, Equifax disseminated the CERT notification internally by email, requesting that applicable personnel responsible for an Apache

---

[43] *Id*.

[44] Russell Grantham, *Equifax, software maker blame each other for opening door to hacks*, THE ATLANTA JOURNAL-CONSTITUTION (updated Sept. 29, 2017), http://www.ajc.com/business/equifax-software-maker-blame-each-other-for-opening-door-hackers/p5wJS5CgTLrmKUL59CTAjM/ (last accessed May 11, 2018).

[45] *Prepared Testimony of Richard F. Smith before the United States House Committee on Energy and Commerce Subcommittee on Digital Commerce and Consumer Protection* (October 3, 2017), https://docs.house.gov/meetings/IF/IF17/20171003/106455/HHRG-115-IF17-Wstate-SmithR-20171003.pdf ("Prepared Testimony of Richard F. Smith, (Oct. 3, 2017)").

Struts installation upgrade the software. The Equifax security department required that patching occur within a 48 hour time period. However, Equifax's IT personnel did not properly utilize this patch, update its software, or otherwise address the vulnerability at that time.[46]

190. Ordinarily, applying a patch that is accompanied by "clear and simple" instructions is a straightforward proposition that provides an easy fix to prevent a serious problem.[47] Had Equifax properly applied the patch like thousands of other affected companies, the vulnerability exploited to perpetrate the breach would have been fixed.[48]

191. The vulnerability and the fact that attackers sought to exploit it was widely publicized. For example, tech blogs reported "a string of attacks that have escalated over the past 48 hours [where] hackers are actively exploiting a critical vulnerability that allows them to take almost complete control of Web servers used

[46] *Id.*

[47] Lily Hay Newman, *Equifax Officially Has No Excuse*, WIRED (Sept. 14, 2017) https://www.wired.com/story/equifax-breach-no-excuse/ (last accessed May 11, 2018).

[48] *Id.*

by banks, government agencies, and large Internet companies."[49] And many sources reported about the uptick in attacks against companies that had not yet installed the patch. Open source security company WhiteSource reported that "[t]he vulnerability was scored as critical (CVSS 10) [the highest grade], mainly due to how easy it is to hack. And indeed reports from days after the Apache Struts March vulnerability was released showed hackers were exploiting it en masse."[50]

192. On March 15, 2017, Equifax ran scans that should have verified that the Apache Struts patch was not properly installed. But Equifax failed to scan all of its systems and failed to discover the vulnerability that still lay at the heart of its systems. This failure to thoroughly scan its systems left Equifax open to the massive breach that would unfold over the next several months.

193. By the admission of Equifax's CEO Richard Smith at the time of the breach, Equifax's systems were infiltrated for the first time on May 13, 2017, well over two months after the Apache Struts patch was first made available.

---

[49] Dan Goodin, *Critical vulnerability under "massive" attack imperils high-impact sites*, ARS TECHNICA (Mar. 9, 2017), https://arstechnica.com/information-technology/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites/ (last accessed May 11, 2018).

[50] Ayala Goldstein, *The Equifax Breach: Who's to Blame?*, WHITESOURCE (Sept. 10, 2017), https://www.whitesourcesoftware.com/whitesource-blog/equifax-data-breach/ (last accessed May 11, 2018).

194. In addition to lacking the necessary safeguards to secure its most valuable "core" data, such as records containing consumer identities and Social Security numbers, Equifax did not have adequate monitoring systems and controls in place to detect the unauthorized infiltration after it occurred. Indeed, Equifax, like any company its size storing valuable data, should have had robust protections in place to detect and terminate a successful intrusion long before access and exfiltration could expand to hundreds of millions of consumer files.

195. Unfortunately Equifax did not have these necessary controls in place, and between May 13 and July 30, 2017, hackers were able to utilize simple commands to determine the credentials of network accounts at Equifax to access and infiltrate the sensitive personal information of approximately 147.9 million American consumers.[51]

Equifax Discovers the Data Breach

196. On July 29, 2017, over four and a half months after the CERT notification about the Apache Struts vulnerability was issued, Equifax's security

[51] AnnaMaria Androitis and Robert McMillan, *Hackers Entered Equifax Systems in March*, THE WALL STREET JOURNAL (updated Sept. 20, 2017), https://www.wsj.com/articles/hackers-entered-equifax-systems-in-march-1505943617 (last accessed May 11, 2018).

team noticed "suspicious network traffic" connected to its consumer dispute website.[52]

197. The security department continued investigating the abnormal activity through July 30, 2017. In response, the Equifax security team deactivated the consumer dispute website and took it entirely offline.

198. Equifax's CEO Richard Smith was informed of the breach the following day on July 31, 2017. Equifax did not notify the chairman of its board of directors until August 22, 2017, and waited two more days to inform the full board.

199. On August 1, 2017, three days after Equifax first noticed the breach, three high-level Equifax executives sold millions of dollars' worth of Equifax stock. Equifax's Chief Financial Officer John Gamble sold $946,374 of stock. Equifax's president of U.S. Information Relations, Joseph Loughran, sold $584,099 of stock. Equifax's President of Workforce Solutions, Rodolfo Ploder, sold $250,458 of stock. And on August 25, 2017, two weeks before Equifax publicly announced the breach, Chief Information Officer Jun Ying sold $950,000 of stock.

[52] See Prepared Testimony of Richard F. Smith (Oct. 3, 2017).

200. None of those transactions were part of previously scheduled 10b5-1 trading plans. Equifax later claimed that these executives did not know of the breach at the time they sold their stock.

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

202. 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. It was determined that Equifax had been subject to cyber-intrusions that resulted in a breach of Equifax's IT systems.

203. In accordance with Equifax's internal policies, the company classified the breach as a "critical incident" and formed a crisis action team, comprised of security, legal, and IT personnel.

204. Equifax designated the response to the breach as "Project Sierra," and instructed those working on Project Sierra that information related to the project was confidential and should not be shared with anyone outside of Equifax's crisis action team.

205. On August 10, 2017, approximately two weeks after discovering the breach, Equifax purchased identity theft security service ID Watchdog for $62 million. ID Watchdog offers services that monitor consumers' credit and warn of potential identity theft for $15 to $25 per month. That same month, well after he was aware of both the Equifax breach and the ID Watchdog acquisition, Equifax CEO Richard Smith touted the acquisition and stated in a speech, "Fraud is a huge opportunity for us—it's a massive, growing business for us."[53]

206. On August 11, 2017, the forensic investigation revealed that certain "dispute documents" submitted by customers to dispute information in their consumer file were accessed, as well as "a large amount" of consumers' personal identifying information and "potentially other data tables."

207. Several days later, Equifax learned through Mandiant that the extensive personal identifying information had not only been accessed but also stolen (*i.e.*, exfiltrated from its systems), and that "large volumes" of consumer data had been compromised.

208. Between August 12 and 15, 2017, Project Sierra team members changed administrative credentials for hundreds of internal databases. The so-

[53] See Puzzanghera, *Senators Slam Equifax.*

called "password reset" required the assistance of a broader group of Equifax IT employees who were not informed of the breach.

209. Equifax also established a notification and remediation plan for the millions of consumers affected by the breach. This effort, which the company designated "Project Sparta," involved setting up a website for consumers to determine whether they were affected by the breach, developing a suite of protective tools for consumers, and staffing call centers.

210. Project Sparta was kept separate from Project Sierra to limit the number of people who knew that Equifax itself had been breached. Those Equifax employees who were only part of Project Sparta were not told that Equifax had been breached, but were instead told that they were assisting with a "business opportunity" whereby Equifax was working for an unnamed client that had experienced a large data breach.

211. Equifax decided to handle much of the work for Project Sparta through its own Global Consumer Solutions business unit, which developed and sold various personal security and identity theft defense products and services to clients.

212. By September 4, 2017, Equifax had compiled a list of the roughly 143 million consumers whose personal information had been stolen. Since that time,

Equifax has identified additional consumer victims. On May 7, 2018, Equifax submitted a "statement for the record" to the Securities and Exchange Commission more fully detailing the breakdown of stolen Personal Information.

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
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

213. As alleged further below, the highly sensitive nature of the Personal Information stolen and unprecedented scale of the breach is likely to affect a significant portion of the U.S. population for years to come.

Equifax's Inadequate Data Security Practices

214. The Equifax breach was the inevitable result of a top-down policy to prioritize growth and profits over data security. The technical deficiencies and

weaknesses that permitted unfettered access to Equifax's systems demonstrate how little priority was given to even rudimentary data security protocols, despite Equifax's role as one of the largest custodians of consumer data in the world.

215. In February 2018, Senator Elizabeth Warren's office released the results of a 5-month investigative report setting forth a number of findings regarding the breach, including Equifax's inadequate data security practices that contributed to the breach (the "Warren Report").

216. The investigation found that "the breach was made possible because Equifax adopted weak cybersecurity measures that failed to protect consumer data – a symptom of what appeared to be the low priority afforded cybersecurity by company leaders. The CEO at the time of the breach, Richard Smith, testified 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 last three years."[54]

217. After consultation with experts, the Warren Report concluded that companies such as Equifax that hold large amounts of sensitive data should have multiple layers of cybersecurity, including (1) frequently updated tools to prevent hackers from breaching their systems; (2) controls that limit hackers' ability to

[54] See Warren Report at 3.

move throughout their systems in the event of an initial breach; (3) restrictions on hackers' ability to access sensitive data in the event of an initial breach; and (4) procedures to monitor and log all unauthorized access in order to stop the intrusion as quickly as possible.[55] The report stated that, "Despite collecting data on hundreds of millions of Americans without their permission, Equifax failed to fully and effectively adopt any of these four security measures."[56]

218. The Warren Report identified six areas where Equifax's cybersecurity measures were particularly deficient:

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 weaknesses through which hackers could gain access." [57]

b. ***Feeble Monitoring of Endpoint and Email Security*** – Endpoint security refers to protecting a corporate network when it is accessed via 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 measures" to secure each endpoint on the network created by these devices. [58]

c. ***Exposure of Sensitive Information*** – Equifax stored and "retained sensitive consumer information on easily accessible systems" rather

[55] *Id.*
[56] *Id.*
[57] *Id.*
[58] *Id.*

than segregating the most sensitive information into locations designed to limit access and maximize security.[59]

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."[60]

e. ***Inadequate Credentialing*** – "Equifax's cybersecurity failures extended to their internal security. Each user on Equifax's system receives a set of privileges. Under a strict security standard, 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 system, 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."[61]

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."[62]

---

[59] *Id.*

[60] *Id.*

[61] *Id.* at 4.

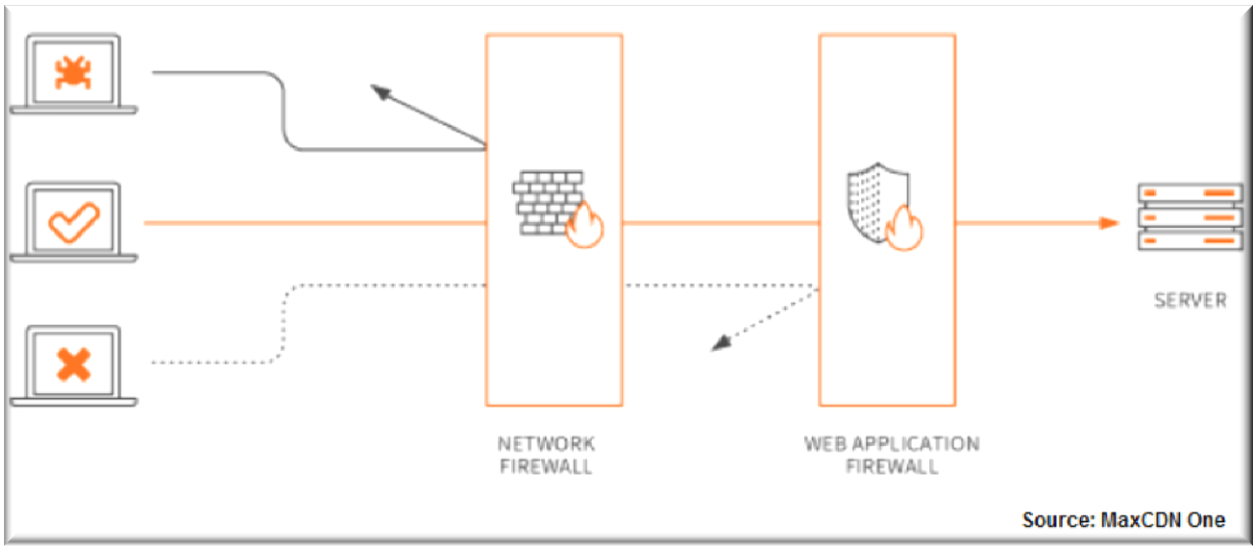
[62] *Id.*

219. 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 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."[63]

220. Other cybersecurity analysists have pointed to additional failures by Equifax. For example, Equifax's consumer dispute website did not make use of a web application firewall ("WAF") that would have served as a second line of defense by intercepting and analyzing all HTTP requests before they reached the web server for processing.[64]

[63] *Id*.

[64] Amos Ndegwa, *What is a Web Application Firewall?*, MAXCDN (May 31, 2016), https://www.maxcdn.com/one/visual-glossary/web-application-firewall/ (last accessed May 11, 2018); Tushar Richabadas, *"WAF Prevents Massive Data Breach at Equifax" . . . The headline that could have been, but wasn't . . ."*, BARRACUDA (Sept. 22, 2017).



221. Because WAFs can detect and stop outside attacks resulting from vulnerabilities inherent in web applications, implementation of a WAF likely would have have prevented the breach from occurring.[65] Equifax's consumer dispute website, contrary to best practices, had no WAF in place at the time of breach.

222. Additionally, there is evidence that Equifax used outdated security certificates, which permitted the hackers to easily bypass Equifax's login protocols, as well as an outdated operating system and infrastructure that was ill-equipped to protect against modern threats. And because Equifax did not have adequate network segmentation, hackers were able to move from the initial point of entry to other IT systems.

[65] *Id.*

223. 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 tens of millions of consumer records. Indeed, any routine and competent monitoring of its consumer dispute portal would have revealed to Equifax that there was significant irregular activity taking place on its servers.

224. Equifax's deficiencies in cybersecurity were well known and widely lamented even within Equifax itself. As one former employee and cybersecurity engineer stated, "The degree of risk [Equifax] assumes is found, by most of the IT staff who worked elsewhere, to be preposterous."[66]

225. Another former Equifax employee involved in a cybersecurity audit of Equifax by Deloitte said, "Nobody took that security audit seriously. Every time there was a discussion about doing something, we had a tough time to get management to understand what we were even asking."[67]

226. The lack of basic safeguards on Equifax's systems and the company's failure to implement even minimal, industry-standard practices further highlights the glaring lack of care exercised by Equifax in protecting its massive trove of

[66] *Id.*
[67] *Id.*

consumer data. Clearly cybersecurity was not a priority at Equifax—even after multiple breaches and warnings had put Equifax on notice that the data it was entrusted to safeguard was extremely vulnerable.

Equifax's Botched Public Disclosure and Response to the Breach

227. Equifax was first warned about the Apache Struts vulnerability on March 8, 2017, the breach occurred on May 13, 2017, and Equifax first observed suspicious network traffic on July 29, 2017. Yet Equifax waited until September 7, 2017, to publicly announce the breach in a nationwide press release. By waiting approximately 7 weeks after Equifax discovered the breach to notify consumers, Equifax deprived consumers of an opportunity to take immediate precautionary measures to protect themselves from identity theft and fraud.

228. Equifax's press release, which did not mention when the breach had occurred, conceded that for 143 million consumers, "[t]he information accessed primarily includes names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers."

229. By using the term "accessed" instead of "stolen" or "exfiltrated", Equifax intentionally failed to convey the seriousness of the breach and that consumers' information was already in the possession of an unauthorized third party.

230. At the time of the announcement, then-CEO Richard Smith wrote that Equifax is "focused on consumer protection and [has] developed a comprehensive portfolio of services to support all U.S. consumers, regardless of whether they were impacted by this incident."

231. Post-breach, Equifax's website contained a link where consumers could provide their last name and the last six digits of their Social Security number to see if their Personal Information was exposed in the breach. This link was circulated by countless online media companies, blogs, and social networks.

232. Contrary to the promises made by Equifax, the website did not indicate whether one's information had been potentially impacted—instead, it told most consumers that they "may" have been compromised.

233. The application then provided consumers with a date in the future when they could enroll in one year of "TrustedID Premier," an Equifax credit monitoring service. However, to sign up for the service, the consumer was required to sign an agreement that included an arbitration clause and class action waiver, and also stated that Equifax could charge the consumer for the year of TrustedID Premier if they did not cancel the service within a year. After a public outcry, Equifax retreated and ultimately removed these requirements from its fine print.

234. Equifax's data breach response website was universally panned not only as unhelpful, but also as a "stalling tactic" and a "sham." According to Brian Krebs, a leading cybersecurity expert:

> As noted in yesterday's breaking story on this breach, the Web site that Equifax advertised as the place where concerned Americans could go to find out whether they were impacted by this breach—equifaxsecurity2017.com—is completely broken at best, and little more than a stalling tactic or sham at worst.
>
> In the early hours after the breach announcement, the site was being flagged by various browsers as a phishing threat. In some cases, people visiting the site were told they were not affected, only to find they received a different answer when they checked the site with the same information on their mobile phones. Others (myself included) received not a yes or no answer to the question of whether we were impacted, but instead a message that credit monitoring service we were eligible for was not available and to check back later in the month. The site asked users to enter their last name and last six digits of their SSN, but at the prompting of a reader's comment I confirmed that just entering gibberish names and numbers produced the same result as the one I saw when I entered my real information: Come back on Sept. 13.[68]

235. In the wake of this problematic rollout, Equifax's website and phone lines crashed repeatedly. The website was overwhelmed, frequently generating system error messages.[69] Numerous consumers had "difficulty in reaching

[68] Brian Krebs, *Equifax Breach Response Turns Dumpster Fire*, KREBS ON SECURITY (Sept. 8, 2017), https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire (last accessed May 11, 2018).
[69] *Id*.

Equifax's call centers and in accessing their security freeze PIN, as well as lengthy hold times, dropped calls, and agents not calling back as promised."[70]

236. There were numerous reports that Equifax's call center representatives did not know how to answer basic questions regarding credit freezes and provided an alternate number to call that did not direct callers to a service that had the answers, but was actually a "triple-X hardcore service."[71]

237. Consumers received different answers as to whether they had been impacted depending on whether they had accessed the site through a computer or mobile device, and the website gave the same information to consumers about whether they had been affected even when they entered incorrect or false information.[72] As recently as April 2018, this Equifax website tool still did not function properly to allow consumers to confirm whether they were victims of the data breach.

---

[70] See Warren Report at 8 (citations and quotations omitted).

[71] Ron Lieber, *How to Protect Yourself After the Equifax Breach*, THE NEW YORK TIMES (updated Oct. 16, 2017), https://www.nytimes.com/interactive/2017/your-money/equifax-data-breach-credit.html (last accessed May 11, 2018) ("Lieber, *How to Protect Yourself After the Equifax Breach*").

[72] Letter from United States House Committee on Energy and Commerce to Richard F. Smith (September 12, 2017), https://schakowsky.house.gov/uploads/Equifax.2017.09.12.Letter%20to%20Equifax%20CEO%20re%20consumer%20data%20breach.%20DCCP.OI.pdf (last accessed May 11, 2018).

238. Richard Smith admitted that Equifax was "disappointed" with the rollout of its website and call centers, and that it "struggled with the initial effort" to assist consumers after the breach.[73]

239. To make matters even worse, the website Equifax set up to help consumers find out whether they were impacted by the breach was itself found to contain security flaws making it vulnerable to hackers. Equifax also directed consumers to a fake phishing site via its official Twitter feed, directing users to check if they had been breached at the website securityequifax2017.com, instead of equifaxsecurity2017.com.

240. The breach led to scammers seeking to take advantage of consumers by sending email phishing scams trying to have already concerned consumers provide important information to other thieves.

241. Scammers were also able to successfully manipulate code on Equifax's website to prompt consumers to download a fraudulent update to Adobe Flash that installs adware, further exposing consumers' information.

[73] Jim Puzzaanghera, *Former Equifax CEO apologizes for data breach and details ways the company messed up*, LOS ANGELES TIMES (Oct. 2, 2017), http://www.latimes.com/business/la-fi-equifax-data-breach-20171002-story.html (last accessed May 11, 2018) ("Puzzaanghera, *Former Equifax CEO apologizes for data breach*").

242. Equifax also attempted to capitalize on the data breach by pushing its own data-protection services,[74] and initially charged many individuals to freeze their own credit files, which were at risk because of Equifax's own negligence.[75]

243. Many consumers who wanted to protect themselves after the breach, but did not want to utilize Equifax products, purchased products and services from "independent" companies like LifeLock, which reported a tenfold increase in enrollment during the month after the Equifax breach.[76] But under questioning, Richard Smith confirmed that LifeLock uses Equifax to monitor its customers' credit and pays Equifax on a per customer basis for use of its services.[77] Thus,

[74] Yuki Noguchi, *After Equifax Hack, Consumers Are On Their Own. Here Are 6 Tips to Protect Your Data*, NATIONAL PUBLIC RADIO (Sept. 14, 2017), http://www.npr.org/2017/09/14/550949718/after-equifax-data-breach-consumers-are-largely-on-their-own (last accessed May 11, 2018) ("Noguchi, *After Equifax Hack, Consumers Are On Their Own*.").

[75] Ron Lieber, *Equifax, Bowing to Public Pressure, Drops Credit-Freeze Fees*, THE NEW YORK TIMES (Sept. 12, 2017), https://www.nytimes.com/2017/09/12/your-money/equifax-fee-waiver.html?rref=collection%2Fbyline%2Fron-lieber&action=click&contentCollection=undefined&region=stream&module=stream_unit&version=latest&contentPlacement=3&pgtype=collection (last accessed May 11, 2018).

[76] See Warren Report at 9.

[77] *Id.*

Equifax stood to *benefit* from the hundreds of thousands of new customers LifeLock received in the aftermath of the breach.[78]

244. Even worse, some Equifax executives sought to personally benefit by avoiding losses relating to the breach. On March 14, 2018, the Securities and Exchange Commission announced it had charged former Equifax CIO Jun Ying with insider trading.[79] The SEC alleged that Ying used insider information to discover that Equifax suffered a data breach, and then sold Equifax stock before the breach was publicly announced—avoiding approximately $117,000 in losses.[80]

[78] Cory Doctorow, *Equifax will make hundreds of millions in extra profits from its apocalyptic breach (forever)*, BOING BOING (Oct. 5, 2017), https://boingboing.net/2017/10/05/failing-up-and-up.html (last accessed May 11, 2018).

[79] Renae Merle, *Former Equifax executive charged with illegally trading before massive data breach was made public*, THE WASHINGTON POST (Mar. 14, 2018), https://www.washingtonpost.com/news/business/wp/2018/03/14/former-equifax-executive-charged-with-insider-trading-ahead-of-data-breach/?utm_term=.cfb0c98b4ca2 (last accessed May 11, 2018).

[80] *Former Equifax Executive Charged With Insider Trading*, U.S. SECURITIES AND EXCHANGE COMMISSION (April 2018), https://www.sec.gov/news/press-release/2018-40 (last accessed May 11, 2018).

245. In September 2017, the FTC stated that it had begun investigating Equifax. Reporters noted that such a disclosure was unusual, as typically the FTC does not discuss open or ongoing investigations.[81]

246. On September 13, 2017, under the headline "Updated information on U.S. website application vulnerability," Equifax posted the following on its website: "Equifax has been intensely investigating the scope of the intrusion with the assistance of a leading, independent cybersecurity firm to determine what information was accessed and who has been impacted. We know that criminals exploited a U.S. website application vulnerability. **The vulnerability was Apache Struts CVE-2017-5638.** We continue to work with law enforcement as part of our criminal investigation, and have shared indicators of compromise with law enforcement." (emphasis added).

247. Apache did not accept the blame, and responded that the breach "was due to [Equifax's] failure to install the security updates provided in a timely

[81] Brian Fung and Hamza Shaban, *The FTC is investigating the Equifax breach. Here's why that's a big deal.*, THE WASHINGTON POST (Sept. 14, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/09/14/the-ftc-confirms-its-investigating-the-equifax-breach-adding-to-a-chorus-of-official-criticism/?utm_term=.e5d4a0a2883a (last accessed May 11, 2018).

manner."[82] On September 15, 2017, Equifax updated its website, and acknowledged Apache's prior alert:

> Questions Regarding Apache Struts
>
> - The attack vector used in this incident occurred through a vulnerability in Apache Struts (CVE-2017-5638), an open-source application framework that supports the Equifax online dispute portal web application.
>
> - Based on the company's investigation, Equifax believes the unauthorized accesses to certain files containing personal information occurred from May 13 through July 30, 2017. The particular vulnerability in Apache Struts was identified and disclosed by U.S. CERT in early March 2017.
>
> - Equifax's Security organization was aware of this vulnerability at that time, and took efforts to identify and to patch any vulnerable systems in the company's IT infrastructure.
>
> - While Equifax fully understands the intense focus on patching efforts, the company's review of the facts is still ongoing. The company will release additional information when available.

248. Since announcing the breach, Equifax has acknowledged on its website the problems relating to its public response to the breach that needed to be fixed, corrected, and clarified. According to the website, "since the announcement, Equifax has taken additional actions including:"

[82] Elizabeth Weise, et al., *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/ (last accessed May 11, 2018).

- Providing a more prominent and clear link from the main www.equifax.com website to the cybersecurity incident website www.equifaxsecurity2017.com, so that consumers can quickly and easily find the information they need.

- Tripling the call center team and continuing to add agents, despite facing some difficulty due to Hurricane Irma.

- Resolving issues with the impact look-up tool.

- Addressing confusion concerning the arbitration and class-action waiver clauses included in the Terms of Use applicable to the product.

- Because of consumer concern, the company clarified that those clauses do not apply to this cybersecurity incident or to the complimentary TrustedID Premier offering.

- The company clarified that the clauses will not apply to consumers who signed up before the language was removed.

- Clarifying that no credit card information is required to sign up for the product and that consumers will not be automatically enrolled or charged after the conclusion of the complimentary year.

- Making changes to address consumer concerns regarding security freezes.

- The company clarified that consumers placing a security freeze will be provided a randomly generated PIN.

- The company continues to work on technical difficulties related to the high volume of security freeze requests.

- Consumers who paid for a security freeze starting at 5pm EST on September 7, 2017 will receive a refund.

- The company agreed to waive fees for removing and placing security freezes through November 21, 2017.[83]

249. On September 26, 2017, Equifax announced that Richard Smith was stepping down as its CEO weeks before he was scheduled to testify before Congress. A New York Times article noted that Smith "presided over a period of rapidly growing sales [at Equifax], driven by expanding troves of sensitive personal data. Profits rose, and the stock price followed. When the crisis hit, the company stumbled. Its website repeatedly crashed as millions of desperate individuals tried to find out whether their information was part of the breach. People who were potentially affected were unable to sign up for protection the company was offering or, even if they had been successful, could not get the service activated. Equifax also charged many people to freeze their credit files before reversing course in the wake of fierce criticism."[84]

[83] https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832 (last accessed May 11, 2018).

[84] Ron Lieber and Stacy Cowley, *Trying to Stem Fallout From Breach, Equifax Replaces C.E.O.*, THE NEW YORK TIMES (Sept. 26, 2017), https://www.nytimes.com/2017/09/26/business/equifax-ceo.html (last accessed May 11, 2018).

250. Richard Smith was replaced by then-interim CEO, Paulino de Rego Barros Jr., who similarly acknowledged that "answers to key consumer questions were too often delayed, incomplete or both."[85]

251. Equifax also confirmed that its Chief Information Officer, Susan Mauldin, and Chief Security Officer, David Webb, were retiring "effective immediately."[86] As noted above, Ms. Mauldin has a bachelor's degree and a master of fine arts degree in music composition. After the breach, Equifax scrubbed its website of information relating to Ms. Mauldin.[87]

252. Equifax has also reportedly pointed fingers at its security consulting partner, Mandiant, claiming that, in the days after the breach, it "sent rookies to look into the vulnerabilities of its systems."[88] On October 2, 2017, Equifax announced that it had identified another 2.5 million people whose Personal

---

[85] See Lieber, *How to Protect Yourself After the Equifax Breach*.

[86] Elizabeth Weise, *A timeline of events surrounding the Equifax data breach*, USA TODAY (Sept. 26, 2017), https://www.usatoday.com/story/tech/2017/09/26/timeline-events-surrounding-equifax-data-breach/703691001/ (last accessed May 11, 2018).

[87] Brett Arends, *Opinion: Equifax hired a music major as chief security officer and she has just retired*, MARKETWATCH (Sept. 15, 2017), http://www.marketwatch.com/amp/story/guid/766FA70C-9A38-11E7-B604-EDFD35AE15F2 (last accessed May 11, 2018).

[88] Jon Fingas, *Equifax breach shows signs of a possible state-sponsored hack*, YAHOO! FINANCE (Sept. 30, 2017), https://finance.yahoo.com/news/equifax-breach-shows-signs-possible-223100521.html (last accessed May 11, 2018).

Information was compromised. The number of known victims increased from 143 million to 145.5 million.[89]

253. On October 3, 2017, former Equifax CEO Richard Smith testified before the House Digital Commerce and Consumer Protection subcommittee. In his testimony, Smith blamed the breach on an "individual" in its technology department who failed to implement the software fixes needed.[90] Apparently this individual "did not ensure communication got to the right person to manually patch the application."[91] Smith also testified that the scanning software Equifax employed to detect such vulnerabilities then also missed this error.[92]

254. Also in early October 2017, the Senate Committee on Banking, Housing and Urban Affairs, and the Senate Committee on the Judiciary, subcommittee on Privacy, Technology, and Law, held hearings regarding the Equifax data breach, at which Smith testified. Smith conceded that neither the

---

[89] Elizabeth Weise and Nathan Bomey, *Equifax breach hit 2.5 million more Americans than first believed*, USA TODAY (Oct. 2, 2017), https://www.usatoday.com/story/tech/2017/10/02/equifax-breach-hit-2-5-million-more-americans-than-first-believed/725100001/ (last accessed May 11, 2018).

[90] Tara Siegel Bernard and Stacy Cowley, *Equifax Breach Caused by Lone Employee's Error, Former C.E.O. Says*, THE NEW YORK TIMES (Oct. 3, 2017), https://www.nytimes.com/2017/10/03/business/equifax-congress-data-breach.html (last accessed May 11, 2018).

[91] *Id.*

[92] *Id.*

Apache Struts vulnerability nor its solution were "novel." He also conceded that fraud would increase after the breach.

255. On February 10, 2018, it was reported, based on a document Equifax turned over to Senate Banking Committee members that Equifax had "disclosed that tax identification numbers, email addresses and phone numbers" were also part of the breach, as well as issuing states for some driver's licenses and credit card expiration.[93]

256. On March 1, 2018, Equifax announced that 2.4 million more Americans were impacted by the data breach than previously disclosed.[94] These additional consumers had names and partial driver's license numbers stolen according to reports. It took approximately 300 days from the time of the breach to

[93] Donna Borak and Kathryn Vasel, *The Equifax hack could be worse than we thought*, CNN MONEY (Feb. 10, 2018), http://money.cnn.com/2018/02/09/pf/equifax-hack-senate-disclosure/index.html (last accessed May 11, 2018); *Equifax Breach Exposed More Consumer Data Than First Disclosed*, INSURANCE JOURNAL (Feb. 13, 2018), https://www.insurancejournal.com/news/national/2018/02/13/480357.htm (last accessed May 11, 2018); Craig Johnson, *Turns out, the Equifax data breach was even worse than we thought*, CLARK (Feb. 14, 2018), https://clark.com/consumer-issues-id-theft/identity-theft/equifax-data-breach-new-revelations-worse/ (last accessed May 11, 2018).

[94] Brian Fung, *Equifax's massive 2017 data breach keeps getting worse*, THE WASHINGTON POST (Mar. 1, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/03/01/equifax-keeps-finding-millions-more-people-who-were-affected-by-its-massive-data-breach/?utm_term=.65d30e38797b (last accessed May 11, 2018).

disclose the existence of these additional 2.4 million victims, and they have still not been individually notified.

257. And it was not until May 7, 2018, when Equifax filed an 8-K Form with the Securities and Exchange Commission, that Equifax finally revealed a full breakdown of the consumer information stolen in the breach.

Data Element Stolen	Standardized Columns Analyzed [1]	Approximate Number of Impacted U.S. Consumers
Name	First Name, Last Name, Middle Name, Suffix, Full Name	146.6 million
Date of Birth	D.O.B.	146.6 million
Social Security Number [2]	SSN	145.5 million
Address Information	Address, Address2, City, State, Zip	99 million
Gender	Gender	27.3 million
Phone Number	Phone, Phone2	20.3 million
Driver's License Number [3]	DL#	17.6 million
Email Address (w/o credentials)	Email Address	1.8 million
Payment Card Number and Expiration Date	CC Number, Exp Date	209,000
TaxID	TaxID	97,500
Driver's License State	DL License State	27,000

258. In all, over 147 million Americans had their Personal Information compromised, nearly all of whom had their name, address, date of birth, and Social Security number stolen as part of the breach.

Equifax Recommends Implementing Credit Freezes

259. The breach forced consumers to spend money to protect themselves, including purchasing products such as credit monitoring and "credit freezes." According to the FTC, a credit freeze, also known as a security freeze, allows a

consumer to restrict access to their credit report, which in turn makes it more difficult for identity thieves to open new accounts in that consumer's name.

260. While credit freezes can be effective in thwarting fraudulent activity, they are also costly, time-consuming, and can create barriers for consumers who are quickly in need of credit. For example, in order to institute a credit freeze, most consumers must pay a fee every time they want to freeze their credit, which can cost up to $10 per freeze depending on state law. If a consumer needs credit while under a credit freeze, she must first unfreeze her credit, again at a cost of up to $10 per unfreeze. The consumer then must pay again to have her credit frozen. Because credit freezes are most effective when they are implemented with all three major CRAs, consumers must pay Equifax, Experian, and TransUnion each time they want to freeze or unfreeze their credit. As Experian's website notes, "Those costs can add up."[95]

261. Credit freezes can also be challenging to implement given that CRAs are notoriously difficult to contact. As noted by a New York Times commenter in the aftermath of the Equifax breach, "Some people are waiting until the middle of

[95] Brian O'Connell, *7 Things You Need to Know Before Freezing Your Credit*, EXPERIAN BLOG (Sept. 20, 2017), https://www.experian.com/blogs/ask-experian/7-things-you-need-to-know-before-freezing-your-credit/ (last accessed May 11, 2018) ("O'Connell, *7 Things You Need to Know Before Freezing Your Credit*").

the night to try to use Equifax's security freeze website and even failing then to get through. It's like trying to get Bruce Springsteen tickets, except nobody wants to see this particular show."[96]

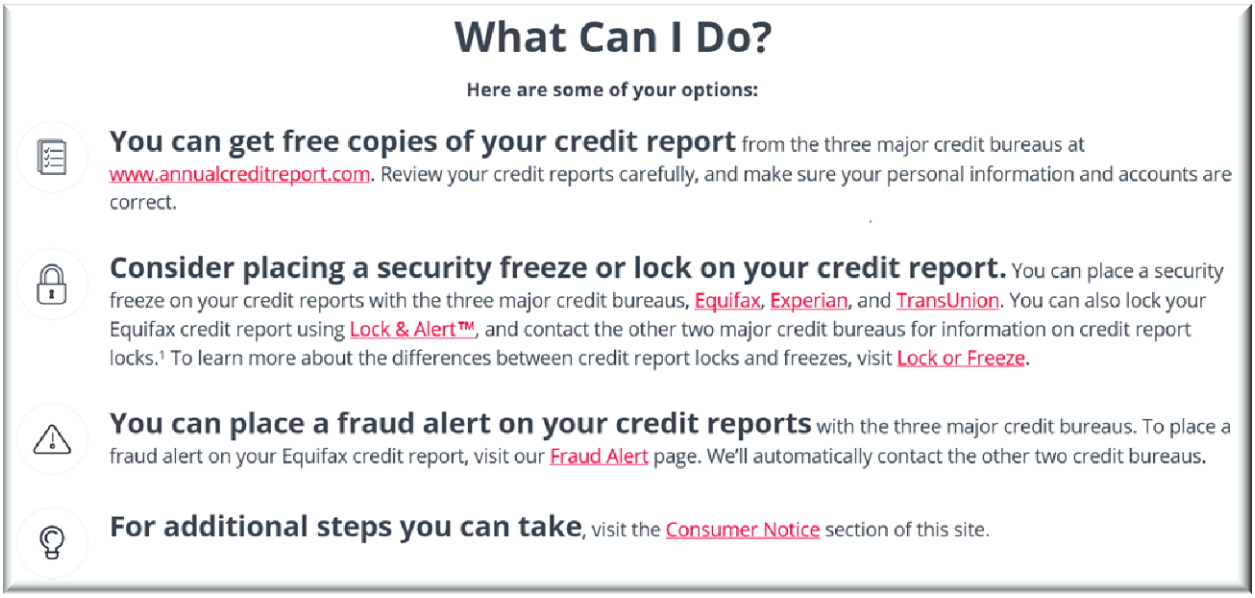
262. Additionally, the lag time associated with freezing and unfreezing credit can create problems when a consumer quickly needs credit, which can make it difficult for consumers to take out loans or make major purchases without planning days or weeks in advance. Experian's website acknowledges that, "Credit freezes can create delays and problems when credit is needed quickly in the case of applying for a loan, credit card, or even a job hunt. . . . During a freeze period, most companies will not extend credit until they check one's credit file with one or three major credit bureaus, and that takes time."[97]

263. Although credit freezes are expensive and can be problematic for those seeking credit, they are among the best defenses to identity theft and fraud, and numerous consumer groups recommended that consumers freeze their credit in the aftermath of the breach. Given the scale of Personal Information compromised in the breach, Equifax itself recommended that consumers freeze their credit to

[96] Ron Lieber, *Finally, Some Answers From Equifax to Your Data Breach Questions*, THE NEW YORK TIMES (Sept. 14, 2017), https://www.nytimes.com/2017/09/14/your-money/equifax-answers-data-breach.html (last accessed May 11, 2018).

[97] See O'Connell, *7 Things You Need to Know Before Freezing Your Credit*.

mitigate possible harm in the aftermath of the breach, placing the following notice on its website:



What Can I Do?

Here are some of your options:

You can get free copies of your credit report from the three major credit bureaus at www.annualcreditreport.com. Review your credit reports carefully, and make sure your personal information and accounts are correct.

Consider placing a security freeze or lock on your credit report. You can place a security freeze on your credit reports with the three major credit bureaus, Equifax, Experian, and TransUnion. You can also lock your Equifax credit report using Lock & Alert™, and contact the other two major credit bureaus for information on credit report locks.[1] To learn more about the differences between credit report locks and freezes, visit Lock or Freeze.

You can place a fraud alert on your credit reports with the three major credit bureaus. To place a fraud alert on your Equifax credit report, visit our Fraud Alert page. We'll automatically contact the other two credit bureaus.

For additional steps you can take, visit the Consumer Notice section of this site.

264. While Equifax agreed to waive fees for implementing credit freezes for a limited period of time (after initially failing to do so), Experian and TransUnion continued to charge consumers full price for the privilege of freezing and unfreezing their credit after the breach.

265. As reported by Krebs on Security, almost 20 percent of Americans froze their credit file as a result of the Equifax breach, costing consumers an

estimated $1.4 billion. A survey conducted by Wakefield Research found that the average cost to consumers who froze their credit was $23.00.[98]

266. On May 9, 2018, Krebs on Security reported that some consumers were still reporting instances of identity theft relating to fraudulent mobile phone accounts being opened in their names, even after implementing credit freezes with the major three CRAs. This type of fraud was possible because many mobile phone merchants do not utilize Equifax, Experian, and TransUnion to process their credit inquiries, but instead they use a relatively obscure CRA known as the National Consumer Telecommunications and Utilities Exchange ("NCTUE").[99]

267. As explained by Krebs, "the NCTUE is a consumer reporting agency founded by AT&T in 1997 that maintains data such as payment and account history, reported by telecommunication, pay TV and utility service providers that are members of NCTUE."[100] After further investigation, Krebs determined that the

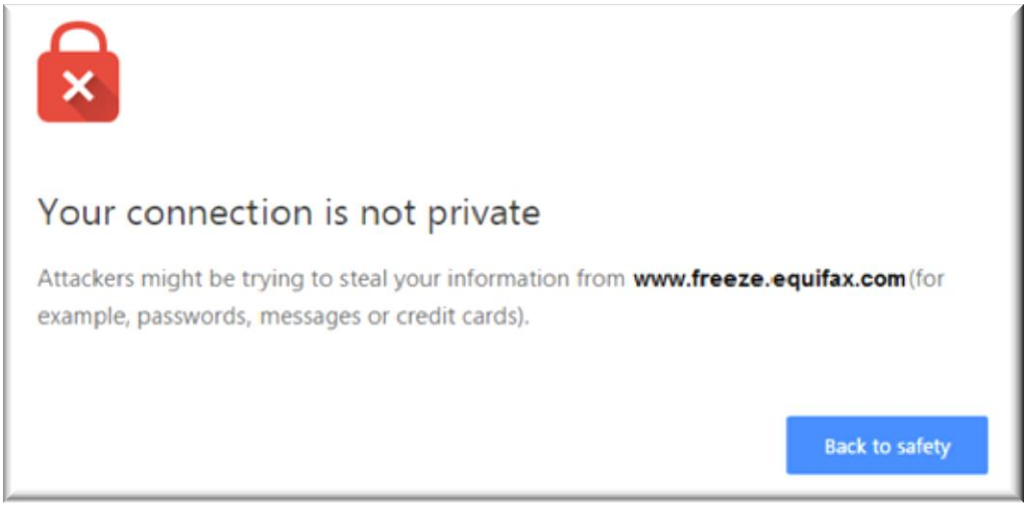
[98] Brian Krebs, *Survey: Americans Spent $1.4B on Credit Freeze Fees in Wake of Equifax Breac*h, KREBS ON SECURITY (Mar. 22, 2018), https://krebsonsecurity.com/2018/03/survey-americans-spent-1-4b-on-credit-freeze-fees-in-wake-of-equifax-breach/ (last accessed May 11, 2018).

[99] Brian Krebs, *Think You've Got Your Credit Freezes Covered? Think Again*, KREBS ON SECURITY (May 9, 2018), https://krebsonsecurity.com/2018/05/another-credit-freeze-target-nctue-com/ (last accessed May 11, 2018).

[100] *Id.*

NCTUE's website is hosted out of Equifax's servers, and Equifax is the sole contractor managing the NCTUE database.[101]

268. As part of his investigation, Krebs visited Equifax's credit freeze application webpage and realized it was using expired SSL certificates (an ongoing problem at Equifax), meaning that users visiting the webpage received a warning that attackers may be able to steal their information by accessing the website. A standard warning of this type appears below:



269. When Krebs visited the NCTUE webpage, he received the same warning. Consequently, not only has Equifax failed to correct its inadequate data security practices post-breach, it also likely dissuaded consumers from taking

[101] *Id.*

advantage of Equifax's (temporarily) free credit freezes for a number of weeks given that they were instructed not to access the website.[102]

270. The problem Equifax's relationship with NCTUE creates is obvious: "Many people who have succeeded in freezing their credit files with Equifax have nonetheless had their identities stolen and new accounts opened in their names thanks to a lesser-known credit bureau that seems to rely entirely on credit checking entities operated by Equifax."[103] Consequently, "Americans are in many cases plunking down $3-$10 per bureau to freeze their credit files, and yet a huge player in this market is able to continue to profit off of identity theft on those same Americans."[104]

271. Equifax attempted to explain away the apparent conflict by issuing a statement providing that the NCTUE is a separate entity, and the NCTUE does not include credit information from Equifax. But as noted above, Equifax listed the NCTUE as one of its primary "assets" in its 2009 Annual Report.

272. Indeed, in its press release regarding the breach, Equifax expressly referred to the NCTUE as one of its "core" databases, stating that "we have found no evidence that this cybersecurity incident impacted *Equifax's core consumer or*

[102] *Id.*

[103] *Id.*

[104] *Id.*

commercial credit reporting databases, including, ACRO, Workforce Solutions, including The Work Number payroll data, *NCTUE*, IXI and CFN." Equifax even sells a product known as "NCTUE Plus", which combines the NCTUE database with Equifax's traditional consumer credit database.[105]

273. Notwithstanding Equifax's attempt to distance itself from another controversy, this report adds to the mounting evidence that Equifax continues to capitalize on and benefit from the breach, while consumers are left with little to no recourse.

Reactions to the Data Breach

274. Reactions to the breach from industry analysts and Congressional members highlight its severity and adverse impact on a significant portion of the U.S. population. Avivah Litam, a fraud analyst at leading information technology consulting and research firm, Gartner, Inc., describing the Equifax breach, said, "[o]n a scale of 1 to 10 in terms of risk to consumers, this a 10."[106]

[105] https://www.equifax.com/business/nctue-plus/ (last accessed May 11, 2018).

[106] Tara Siegel Bernard, et al., *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, THE NEW YORK TIMES (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html?mcubz=3 (last accessed May 11, 2018) ("Bernard, et al., *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*").

275. Senator Mark Warner of Virginia stated, "It is no exaggeration to suggest that a breach such as this—exposing highly sensitive Personal Information central for identity management and access to credit—represents a real threat to the economic security of Americans."[107]

276. Massachusetts Attorney General Maura Healey called the Equifax data breach "the most brazen failure to protect consumer data we have ever seen."[108] Another commenter noted that the Equifax breach "will go down as one of the worst data breaches in history, and could prove to be the most damaging ever for American consumers."[109]

277. In February 2018, Equifax was ranked as the No. 1 "Most Hated Company in America", beating out dozens of bad reputation challengers including

[107] Craig Timberg, et al., *Data of 143 million Americans – nearly half the country – exposed in Equifax hack*, CHICAGO TRIBUNE (Sept. 8, 2017), http://www.chicagotribune.com/business/national/ct-equifax-data-breach-20170907-story.html (last accessed May 11, 2018).

[108] See Noguchi, *After Equifax Hack, Consumers Are On Their Own.*

[109] *Equifax breach could be worst in history*, SCOTSMAN GUIDE (Sept. 11, 2017), https://www.scotsmanguide.com/News/2017/09/Equifax-breach-could-be-worst-in-history/ (last accessed May 11, 2018).

the NFL (No. 3), Wells Fargo (No. 11), Comcast (No. 15), Monsanto (No. 16) and The Weinstein Company (No. 20).[110]

278. In written testimony for his hearing with the House Energy and Commerce Committee, former Equifax CEO Richard Smith stated, "Equifax was entrusted with Americans' private data and we let them down," acknowledged the "human error" involved, and said that "[t]he company failed to prevent sensitive information from falling into the hands of wrongdoers."[111]

279. Perhaps most significantly, consumers have no way of "opting out" of Equifax's data collection or hindering Equifax's ability to profit from the sale of such information.[112] During his testimony before the United States Senate, Equifax's former CEO testified that he did not think that people should be able to delete their data from Equifax's systems.[113]

---

[110] Samuel Stebbins, et al., *Bad reputation: America's Top 20 most-hated companies*, USA TODAY (Feb. 12, 2018), https://www.usatoday.com/story/money/business/2018/02/01/bad-reputation-americas-top-20-most-hated-companies/1058718001/ (last accessed May 11, 2018).

[111] See Puzzaanghera, *Former Equifax CEO apologizes for data breach*.

[112] Ron Lieber, *'Dear Equifax: You're Fired.' If Only It Were That Easy.*, THE NEW YORK TIMES (Oct. 6, 2017), https://www.nytimes.com/2017/10/06/your-money/credit-scores/equifax-hack.html (last accessed May 11, 2018).

[113] *Id.*

280. As referenced above, in February 2018, Senator Elizabeth Warren's office released a 15-page report summarizing its findings after a multi-month investigation that included questioning Equifax executives in Senate hearings, consulting outside experts, and sending letters containing dozens of questions to Equifax, federal regulators, and other credit rating agencies. In addition to the findings summarized above relating to Equifax's inadequate data security practices, the Warren Report concluded that:

a. ***Equifax Set up a Flawed System to Prevent and Mitigate Data Security Problems***. The breach was made possible because Equifax adopted weak cybersecurity measures that did not adequately protect consumer data. The company failed to prioritize cybersecurity and failed to follow basic procedures that would have prevented or mitigated the impact of the breach. For example, Equifax was warned of the vulnerability in the web application software Apache Struts that was used to breach its system, and emailed staff to tell them to fix the vulnerability – but then failed to confirm that the fixes were made. Subsequent scans only evaluated part of Equifax's system and failed to identify that the Apache Struts vulnerability had not been remediated.

b. ***Equifax Ignored Numerous Warnings of Risks to Sensitive Data***. Equifax had ample warning of weaknesses and risks to its systems. Equifax received a specific warning from the Department of Homeland Security about the precise vulnerability that hackers took advantage of to breach the company's systems. The company had been subject to several smaller breaches in the years prior to the massive 2017 breach, and several outside experts identified and reported weaknesses in Equifax's cyber defenses before the breach occurred. But the company failed to heed – or was unable to effectively heed – these warnings.

c. ***Equifax Failed to Notify Consumers, Investors, and Regulators about the Breach in a Timely and Appropriate Fashion***. The breach occurred on May 13, 2017, and Equifax first observed suspicious signs of a problem on July 29, 2017. But Equifax failed to notify consumers, investors, business partners, and the appropriate regulators until 40 days after the company discovered the breach. By failing to provide adequate information in a timely fashion, Equifax robbed consumers of the ability to take precautionary measures to protect themselves, materially injured investors and withheld market-moving information, and prevented federal and state governments from taking action to mitigate the impacts of the breach.

d. ***Equifax Took Advantage of Federal Contracting Loopholes and Failed to Adequately Protect Sensitive IRS Taxpayer Data***. Soon after the breach was announced, Equifax and the IRS were engulfed in controversy amid news that the IRS was signing a new $7.2 million contract with the company. Senator Warren's investigation revealed that Equifax used contracting loopholes to force the IRS into signing this "bridge" contract, and the contract was finally cancelled weeks later by the IRS after the agency learned of additional weaknesses in Equifax security that potentially endangered taxpayer data.

e. ***Equifax's Assistance and Information Provided to Consumers Following the Breach was Inadequate***. Equifax took 40 days to prepare a response for the public before finally announcing the extent of the breach – and even after this delay, the company failed to respond appropriately. Equifax had an inadequate crisis management plan and failed to follow their own procedures for notifying consumers. Consumers who called the Equifax call center had hours-long waits. The website set up by Equifax to assist consumers was initially unable to give individuals clarity other than to tell them that their information "may" have been hacked – and that website had a host of security problems in its own right. Equifax delayed their public notice in part because the company spent almost two weeks trying to determine precisely which consumers were affected by the breach – but then failed to provide consumers with any specific information to determine if their data was breached. And while Equifax continues to publicly state only that data was "accessed," the

> company has confirmed that the data was exfiltrated – stolen – from their systems and downloaded by the hackers. Equifax appeared to be more focused on using the breach as a profitmaking opportunity for other company services rather than providing redress to consumers.[114]

281. The Warren Report concluded that "Equifax and other credit reporting agencies have taken advantage of consumers for years, collecting their data without permission and turning a huge profit while failing to adequately protect that data." The report recommended that federal legislation be enacted to force "Equifax and its peers to put appropriate emphasis on protecting consumer data."[115]

Aftermath of the Breach: Consequences for Consumers and the Economy

282. The effects of the Equifax breach on consumers are severe. More than just a one-time occurrence, the identities of affected individuals are now permanently compromised. Identity thieves can use the information exfiltrated in the breach to perpetrate a wide variety of crimes at the expense of the victims of the Equifax breach, including tax fraud; identity theft; opening fraudulent credit cards and loan accounts; defrauding the government, such as by changing immigration status using the victim's name, obtaining a driver's license or identification card in the victim's name but with another's picture, or using the

[114] See Warren Report at 2.
[115] *Id*. at 11.

victim's information to obtain government benefits; obtaining a job in the victim's name; procuring housing using a false identity; or even giving false information to police during an arrest. In the medical context, consumers' stolen Personal Information can be used to submit false insurance claims, obtain prescription drugs or medical devices for black-market resale, or get medical treatment in the victim's name.

283. With all of the data that was exfiltrated in the Equifax breach, hackers will have "a greater chance of successfully committing financial crimes" against innocent victims—"open[ing] the door for total identity theft."[116]

284. There is a report that information from the Equifax data breach is already for sale on one such black market, known as the "dark web."[117] And as set forth above, consumers have collectively spent millions or more paying for mitigation measures like credit monitoring and credit freezes in the aftermath of the breach.

---

[116] Adam Shell, *Equifax data breach could create lifelong identity theft threat*, USA TODAY (Sept. 9, 2017), https://www.usatoday.com/story/money/2017/09/09/equifax-data-breach-could-create-life-long-identity-theft-threat/646765001/ (last accessed May 11, 2018).

[117] Jeff John Roberts, *Why Equifax Executives Will Get Away With the Worst Data Breach in History*, FORTUNE (Sept. 16, 2017), http://fortune.com/2017/09/16/equifax-legal/?iid=sr-link3 (last accessed May 11, 2018).

285. Additionally, the risk of Social Security, VA benefits, and other benefits fraud is increased. For example, veterans can currently change their VA benefit deposit account with a form that includes their Social Security number.[118]

286. There also may be national security implications to the breach: it is easier to locate individuals operating in the intelligence community and to detect if those individuals are financially vulnerable.[119]

287. Annual monetary losses from identity theft are in the billions of dollars. According to a Presidential Report on identity theft produced in 2007:

> In addition to the losses that result when identity thieves fraudulently open accounts . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.

---

[118] Michelle Singletary, *If you expect to get Social Security, this is the one thing you need to do in the aftermath of the Equifax data breach*, THE WASHINGTON POST (Oct. 2, 2017), https://www.washingtonpost.com/news/get-there/wp/2017/10/02/if-you-expect-to-get-social-security-this-is-the-one-thing-you-need-to-do-in-the-aftermath-of-the-equifax-data-breach/?utm_term=.3012a9bf9519 (last accessed May 11, 2018); *Duckworth Slams Equifax CEO For Failing To Safeguard Veterans' Personal Information* (Nov. 9, 2017), https://www.duckworth.senate.gov/news/press-releases/duckworth-slams-equifax-ceo-for-failing-to-safeguard-veterans-personal-information (last accessed May 11, 2018).

[119] See Bernard, et al., *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*

> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[120]

288. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[121]

289. The unauthorized disclosure of Social Security Numbers can be particularly damaging because Social Security Numbers cannot easily be replaced. In order to obtain a new number, a person must prove, among other things, he or she continues to be disadvantaged by the misuse. Thus, under current rules, no new number can be obtained until the damage has been done. Furthermore, as the Social Security Administration warns:

---

[120] http://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf, at 11(last accessed May 11, 2018).

[121] Report to Congressional Requesters, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007) at 29, http://www.gao.gov/new.items/d07737.pdf (last accessed May 11, 2018).

> A new number probably will not solve all your problems. This is because other governmental agencies (such as the Internal Revenue Service and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Also, because credit reporting companies use the number, along with other Personal Information, to identify your credit record, using a new number will not guarantee you a fresh start. This is especially true if your other Personal Information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you will not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit card information is not associated with the new number, the absence of any credit history under the new number may make it more difficult for you to get credit.[122]

290. Personal Information such as that stolen in the Equifax data breach is highly coveted by, and a frequent target of, hackers.

- Thieves use the credit card information to create fake credit cards that can be swiped and used to make purchases as if they were the real credit cards;
- Thieves reproduce stolen debit cards and use them to withdraw cash from ATMs;
- Thieves can use the victim's Personal Information to commit immigration fraud, obtain a driver's license or identification card in the victim's name but with another's picture, use the victim's information to obtain government benefits, or file a fraudulent tax return using the victim's information to obtain a fraudulent refund; or get medical services using consumers' stolen information or commit any number of

[122] *Identity Theft and Your Social Security Number* (June 2017) at 6, http://www.ssa.gov/pubs/10064.html (last accessed May 11, 2018).

other frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest.

291. Equifax has consciously worked to assemble a massive stash of private employment and salary history information, information that is now exposed and susceptible to use by bad actors.[123]

292. Specifically, because homebuyers and mortgage applicants tend to have significant information on file with credit bureaus, they are especially at risk for identity theft after the Equifax data breach. Identity theft during an important purchase like buying a home is particularly devastating and creates significant legal and financial issues.[124]

293. A cyber black market exists in which criminals openly post and sell stolen credit card numbers, Social Security numbers, and other Personal Information on a number of Internet websites.

294. Equifax's actions and failures to act when required have caused Plaintiffs and the Class defined below to suffer harm and/or face the significant and imminent risk of future harm, including:

[123] See Krebs, *Equifax Breach Fallout: Your Salary History*.

[124] Kenneth R. Harney, *Theft of Equifax data could lead to years of grief for home buyers and mortgage applicants*, THE WASHINGTON POST (Sept. 13, 2017), https://www.washingtonpost.com/realestate/theft-of-data-could-lead-to-years-of-grief-for-home-buyers-and-mortgage-applicants/2017/09/12/ed0f66fc-971a-11e7-82e4-f1076f6d6152_story.html (last accessed May 11, 2018).

a. theft of their Personal Information;

b. costs associated with requested credit freezes;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. costs associated with purchasing credit monitoring and identity theft protection services;

e. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Equifax data breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

h. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being placed in the hands of criminals;

i. damages to and diminution in value of their Personal Information entrusted, directly or indirectly, to Equifax with the mutual understanding that Equifax would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others;

j. continued risk of exposure to hackers and thieves of their Personal Information, which remains in Equifax's possession and is subject to

further breaches so long as Equifax fails to undertake appropriate and adequate measures to protect Plaintiffs and the Class; and

k. for purchasers' of Equifax's own credit monitoring and identity theft protection products, diminution of the value and/or loss of the benefits of those products.

295. Consequently, victims of the Equifax breach are at an imminent risk of fraud and identity theft for years to come.

CLASS ACTION ALLEGATIONS

296. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of the following nationwide class (the "Nationwide Class" or the "Class"):

NATIONWIDE CLASS

All natural persons residing in the United States whose Personal Information was compromised as a result of the data breach announced by Equifax on or about September 7, 2017, as identified by Equifax's records relating to that data breach.

The Nationwide Class asserts claims against Equifax for violation of the FCRA (Count 1), negligence (Count 2), negligence *per se* (Count 3), violation of Georgia's Fair Business Practices Act (Count 4), and unjust enrichment (Count 5). The Nationwide Class also requests a declaratory judgment (Count 6).

297. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of state-by-state claims in the alternative to the nationwide claims brought under Georgia common law, as well as statutory claims

under state data breach statutes and consumer protection statutes (Counts 10 through 99, and Count 4 in the alternative to the nationwide claim under the Georgia Fair Business Practices Act), on behalf of separate statewide subclasses for each State, the District of Columbia, Puerto Rico, and the Virgin Islands (the "Statewide Subclasses"), defined as follows:

STATEWIDE [NAME OF STATE OR TERRITORY] SUBCLASS

All natural persons residing in [name of state or territory] whose Personal Information was compromised as a result of the data breach announced by Equifax on or about September 7, 2017, as identified by Equifax's records relating to that data breach.

298. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of a subclass comprised of Equifax customers who allege that Equifax breached actual and implied contracts to adequately protect their Personal Information (Counts 7 and 8), referred to as the "Equifax Contract Subclass" and described more specifically as follows:

NATIONWIDE EQUIFAX CONTRACT SUBCLASS

All natural persons residing in the United States (1) whose Personal Information was compromised as a result of the data breach announced by Equifax on or about September 7, 2017, as identified by Equifax's records relating to that data breach, and (2) who purchased or received for consideration Equifax credit monitoring or identity theft protection products, or who otherwise, subject to the Equifax Privacy Policy, transmitted directly to Equifax any of their Personal Information.

299. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), in the alternative to the nationwide claims of the Equifax Contract Subclass, Plaintiffs seek certification of separate statewide subclasses for each State, the District of Columbia, Puerto Rico, and the Virgin Islands (the "Equifax Contract Statewide Subclasses"), comprised of those who allege that Equifax breached actual and implied contracts to adequately protect their Personal Information and more specifically defined as follows:

EQUIFAX CONTRACT STATEWIDE [NAME OF STATE OR TERRITORY] SUBCLASS

> **All natural persons residing in [name of state or territory] (1) whose Personal Information was compromised as a result of the data breach announced by Equifax on or about September 7, 2017, as identified by Equifax's records relating to that data breach, and (2) who purchased or received for consideration Equifax credit monitoring or identity theft protection products, or who otherwise, subject to the Equifax Privacy Policy, transmitted directly to Equifax any of their Personal Information.**

300. Pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3), as applicable, and (c)(4), Plaintiffs seek certification of a subclass comprised of those who claim that Equifax violated the consumer report disclosure requirements of the FCRA, 15 U.S.C. § 1681g(a) (Count 9), which is referred to as the "FCRA Disclosure Subclass" and is more specifically defined as follows:

FCRA DISCLOSURE SUBCLASS

All natural persons residing in the United States (1) whose Personal Information was compromised as a result of the data breach announced by Equifax on or about September 7, 2017, as identified by Equifax's records relating to that data breach, and (2) who requested and obtained their consumer file from Equifax from July 29, 2017 through the present.

301. 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.

302. **Numerosity: Federal Rule of Civil Procedure 23(a)(1)**. The members of each Class and Subclass are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. Plaintiffs are informed and believe—based upon Equifax's press releases and securities filings—that there are approximately 147,900,000 class members. Those individuals' names and addresses are available from Equifax's records, and Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods. On information and belief, there are at least thousands of

class members in each Subclass, making joinder of all Subclass members impracticable.

303. **Commonality and Predominance: Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3)**. As to each Class and Subclass, this action involves common questions of law and fact, which predominate over any questions affecting individual class members, including:

a. Whether Equifax knew or should have known that its computer systems were vulnerable to attack;

b. Whether Equifax failed to take adequate and reasonable measures to ensure its data systems were protected;

c. Whether Equifax failed to take available steps to prevent and stop the breach from happening;

d. Whether Equifax failed to disclose the material facts that it did not have adequate computer systems and security practices to safeguard consumers' Personal Information;

e. Whether Equifax failed to provide timely and adequate notice of the data breach;

f. Whether Equifax owed a duty to Plaintiffs and Class and Subclass members to protect their Personal Information and to provide timely and accurate notice of the data breach to Plaintiffs and Class and Subclass members;

g. Whether Equifax breached its duties to protect the Personal Information of Plaintiffs and Class and Subclass members by failing to provide adequate data security and by failing to provide timely and accurate notice to Plaintiffs and Class and Subclass members of the data breach;

h. Whether Equifax's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the unauthorized access and/or theft of tens of millions of consumers' Personal Information;

i. Whether Equifax's conduct amounted to violations of the FCRA (15 USC §§ 1681, *et seq.*), state consumer protection statutes, and/or state data breach statutes;

j. Whether Equifax's conduct renders it liable for negligence, negligence *per se*, unjust enrichment, breach of contract, and/or breach of implied contract;

k. Whether, as a result of Equifax's conduct, Plaintiffs and Class and Subclass members face a significant threat of harm and/or have already suffered harm, and, if so, the appropriate measure of damages to which they are entitled; and

l. Whether, as a result of Equifax's conduct, Plaintiffs and Class and Subclass members are entitled to injunctive, equitable, declaratory and/or other relief, and, if so, the nature of such relief.

304. **Typicality: Federal Rule of Civil Procedure 23(a)(3)**. As to each Class and Subclass, Plaintiffs' claims are typical of other Class members' claims because Plaintiffs and Class members were subjected to the same allegedly unlawful conduct and damaged in the same way.

305. **Adequacy of Representation: Federal Rule of Civil Procedure 23(a)(4)**. Plaintiffs are adequate class representatives because their interests do not conflict with the interests of Class members who they seek to represent, Plaintiffs have retained counsel competent and experienced in complex class action litigation and data breach litigation, and Plaintiffs intend to prosecute this action vigorously. The Class members' interests will be fairly and adequately protected by Plaintiffs and their counsel.

306. **Declaratory and Injunctive Relief: Federal Rule of Civil Procedure 23(b)(2)**. 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. Equifax has acted and/or refused to act on grounds generally applicable to the Class, making final injunctive relief or corresponding declaratory relief appropriate.

307. **Superiority: Federal Rule of Civil Procedure 23(b)(3)**. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Equifax, so it would be impracticable for Class members to individually seek redress for Equifax's wrongful conduct. Even if Class members could afford litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and

expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

CHOICE OF LAW FOR NATIONWIDE CLAIMS

308. 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.

309. The principal place of business of Equifax, located at 1550 Peachtree Street NE, 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.

310. Equifax's response to the data breach at issue here, and corporate decisions surrounding such response, were made from and in Georgia.

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

312. 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.

313. 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's Fair Business Practices Act may be applied to non-resident consumer plaintiffs.

CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT 1

VIOLATION OF THE FAIR CREDIT REPORTING ACT, 15 U.S.C. §§ 1681, *et seq*.

On Behalf of Plaintiffs and the Nationwide Class

314. Plaintiffs repeat and reallege Paragraphs 1-313, as if fully alleged herein.

315. Plaintiffs specifically restate the allegations of Paragraphs 109-121, relating to each Defendant's status and operation as a CRA for purposes of the FCRA.

316. Equifax is a CRA—a "consumer reporting agency" and a "consumer reporting agency that compiles and maintains files on consumers on a nationwide basis" as defined in 15 U.S.C. §§ 1681a(f) and (p), respectively.

317. As individuals, Plaintiffs and Class members are consumers entitled to the protections of the FCRA. 15 U.S.C. § 1681a(c).

318. Equifax compiled and maintained a "consumer report" on Plaintiffs and Class members, as defined in 15 U.S.C. § 1681a(d): any "written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for—(A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 1681b of this title."

319. The compromised data was a consumer report under the FCRA because it was a communication of information bearing on Class members' credit

worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living used, or expected to be used or collected in whole or in part, for the purpose of serving as a factor in establishing Class members' eligibility for credit.

320. As a CRA, Equifax may only furnish a consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b, "and no other." 15 U.S.C. § 1681b(a). None of the purposes listed under section 1681b permit CRAs to furnish consumer reports to unauthorized or unknown entities, or computer hackers such as those who accessed Class members' Personal Information.

321. Equifax furnished Class members' consumer reports, in violation of section 1681b, by disclosing those consumer reports to unauthorized entities and computer hackers, and by allowing unauthorized entities and computer hackers to access their consumer reports.

322. The FCRA requires Equifax, as a CRA, to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title." 15 U.S.C. § 1681e(a).

323. The Federal Trade Commission has pursued enforcement actions against CRAs under the FCRA for failing to "take adequate measures to fulfill

their obligations to protect information contained in consumer reports, as required by the" FCRA, in connection with data breaches.

324. Equifax failed to maintain reasonable procedures designed to limit the furnishing of Class members' consumer reports to permitted purposes, and/or failed to take adequate security measures that would prevent disclosure of Class members' consumer reports to unauthorized entities or computer hackers.

325. As alleged in detail herein, Equifax's security practices and procedures were so severely deficient or nonexistent, despite its knowledge that this Personal Information was coveted by attackers and certain to be subject to attempted hacks and exfiltration, that Equifax in fact voluntarily and for all practical purposes knowingly offered, provided, and furnished this information to unauthorized third parties.

326. As a direct and proximate result of Equifax's actions and failures to act described herein, and utter failure to take adequate and reasonable measures to ensure its data systems were protected, Equifax offered, provided, and furnished Plaintiffs' and Class members' consumer reports to unauthorized third parties.

327. Equifax's disclosure of consumer reports under these circumstances was not permitted by, and thus was in violation of, Sections 1681b and 1681e of the FCRA.

328. As a direct and proximate result of Equifax's actions and failures to act described herein, and its violation of the FCRA, Plaintiffs and Class members have suffered harm and/or face the significant risk of harm suffering such harm in the future, all as described above.

329. Under Section 1681o of the FCRA, Equifax is liable to Plaintiffs and Class members for negligently failing to comply with the requirements that a CRA not disclose consumer reports and take measures designed to avoid the unauthorized disclosure of consumer reports. Equifax therefore is liable to Plaintiffs and Class members for their actual damages as a result of Equifax's failure to comply with the FCRA, as well as costs and reasonable attorneys' fees, in amounts to be proven at trial.

330. In addition, Equifax's failure to comply with the foregoing requirements was willful because Equifax knew or should have known, but recklessly disregarded, that its cybersecurity measures were inadequate and unreasonable and additional steps were necessary to protect consumers' Personal Information from security breaches. The willful and reckless nature of Equifax's violations is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, Equifax's numerous other data breaches in the past, Equifax's knowledge of numerous other

previous high-profile data breaches, and warnings from cybersecurity experts. Further, Equifax touts itself as an industry leader in breach prevention; thus, Equifax was well aware of the importance of the measures organizations should take to prevent data breaches, and willingly failed to take them.

331. Equifax also acted willfully and recklessly because, as a CRA, it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. *See, e.g.*, 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary On The Fair Credit Reporting Act. 16 C.F.R. Part 600, Appendix To Part 600, Sec. 607 2E. Equifax obtained or had available these and other substantial written materials that apprised them of their duties under the FCRA. Nonetheless, by its utter failure to meet its acknowledged responsibilities and known duties regarding the need to adopt adequate data security measures, Equifax acted consciously in depriving Plaintiffs and Class members of their rights under the FCRA.

332. Therefore, Equifax is liable to Plaintiffs and Class members in an amount equal to actual damages, or damages of not less than $100 and not more than $1,000 for each Plaintiff and Class member, as well as punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a).

COUNT 2

NEGLIGENCE

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

333. Plaintiffs repeat and reallege Paragraphs 1-313, as if fully alleged herein.

334. Equifax owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their Personal Information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing Equifax's security systems to ensure that Plaintiffs' and Class members' Personal Information in Equifax's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

335. Equifax's duty to use reasonable care arose from several sources, including but not limited to those described below.

336. Equifax had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiffs and Class Members would be harmed by the failure to protect their Personal Information because hackers routinely attempt to steal such information and use it for nefarious purposes, Equifax knew that it was more likely than not Plaintiffs and other Class members would be harmed.

337. Equifax's duty also arose under Section 5 of the Federal Trade Commission Act ("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 failing to use reasonable measures to protect Personal Information by companies such as Equifax. Various FTC publications and data security breach orders further form the basis of Equifax's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

338. Equifax's duty also arose from Equifax's unique position as one of three nationwide credit-reporting companies that serve as linchpins of the financial system. Equifax undertakes its collection of highly sensitive information generally without the knowledge or consent of consumers and consumers cannot "opt out" of

Equifax's data collection activities. Equifax holds itself out as a trusted steward of consumer data, and thereby assumes a duty to reasonably protect that data. The consumer public and, indeed, all those who participate in modern American economic life collectively repose a trust and confidence in Equifax to perform that stewardship carefully. Otherwise consumers would be powerless to fully protect their interests with regard to their Personal Information, which is controlled by Equifax. Because of its crucial role within the credit system, Equifax was in a unique and superior position to protect against the harm suffered by Plaintiffs and Class members as a result of the Equifax data breach.

339. Equifax admits that it has an enormous responsibility to protect consumer data, that it is entrusted with this data, and that it did not live up to its responsibility to protect the Personal Information at issue here.

340. Equifax's duty also is based on the FCRA, which reflects Congress's considered judgment that CRAs such as Equifax hold a unique and superior position in our credit economy, a position that if abused would foreseeably and probably injure consumers like Plaintiffs and Class members. The FCRA thus requires that Equifax maintain reasonable procedures designed to avoid unauthorized release of information contained in consumer reports, and requires that when issued, consumer reports are complete and accurate.

341. Equifax also acknowledges and recognizes a pre-existing duty to exercise reasonable care to safeguard Plaintiffs' and Class members' Personal Information that extends to those who are entrusted with such information. Equifax may now deny that it has any legal duty to protect information relating to the data *Equifax* maintains relating to Plaintiffs and Class Members. But when dealing with businesses that purchase consumer information *from Equifax*, Equifax explicitly recognizes and contractually insists that those businesses have a duty to protect this information. For example, in its form Broker Subscription Agreement, Equifax requires that:

- "only Authorized Users can order or have access to" protected information;
- credit reports are not provided "to any third party except as permitted";
- protected information "must be encrypted when not in use and all printed [protected information] must be stored in a secure, locked container when not in use, and must be completely destroyed when no longer needed by cross-cut shredding machines (or other equally effective destruction method) such that the results are not readable or useable for any purpose";

- protected information must be encrypted with: "Advanced Encryption Standard (AES), minimum 128-bit key or Triple Data Encryption Standard (3DES), minimum 168-bit key, encrypted algorithms";
- Equifax's business partner must "monitor compliance" with these obligations "and immediately notify EQUIFAX if [the business partner] suspects or knows of any unauthorized access or attempt to access the" protected information;
- Equifax's business partner must "not ship hardware or software . . . to third parties without deleting . . . any consumer information";
- Equifax's business partner must "use commercially reasonable efforts to assure data security when disposing of any consumer report information";
- "Such efforts must include the use of those procedures issued by" applicable federal agencies, "e.g. the Federal Trade Commission . . . ."

342. With regard to network security, Equifax further acknowledges and requires that its business partners must "use commercially reasonable efforts to protect EQUIFAX Information when stored on servers, subject to the following requirements":

- "EQUIFAX Information must be protected by multiple layers of network security, including but not limited to, firewalls, routers, intrusion detection device";
- "secure access (both physical and network) to systems storing EQUIFAX Information must include authentication and passwords that are changed at least every 90 days";
- "all servers must be kept current and patched on a timely basis with appropriate security-specific system patches, as they are available."

343. Equifax also had a duty to safeguard the Personal Information of Plaintiffs and Class members and to promptly notify them of a breach because of state laws and statutes that require Equifax to reasonably safeguard sensitive Personal Information, as detailed herein.

344. Timely notification was required, appropriate and necessary so that, among other things, Plaintiffs and Class members could take appropriate measures to freeze or lock their credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or

debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by Equifax's misconduct.

345. Equifax breached the duties it owed to Plaintiffs and Class members described above and thus was negligent. Equifax breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the Personal Information of Plaintiffs and Class members; (b) detect the breach while it was ongoing; (c) maintain security systems consistent with industry standards; and (d) disclose that Plaintiffs' and the Class members' Personal Information in Equifax's possession had been or was reasonably believed to have been, stolen or compromised.

346. But for Equifax's wrongful and negligent breach of its duties owed to Plaintiffs and Class members, their Personal Information would not have been compromised.

347. As a direct and proximate result of Equifax's negligence, Plaintiffs and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial. Plaintiffs' and Class members' injuries include:

a. theft of their Personal Information;

b. costs associated with requested credit freezes;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. costs associated with purchasing credit monitoring and identity theft protection services;

e. unauthorized charges and loss of use of and access to their financial account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Equifax data breach—including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

h. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their Personal Information being placed in the hands of criminals;

i. damages to and diminution in value of their Personal Information entrusted, directly or indirectly, to Equifax with the mutual understanding that Equifax would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others;

j. continued risk of exposure to hackers and thieves of their Personal Information, which remains in Equifax's possession and is subject to further breaches so long as Equifax fails to undertake appropriate and adequate measures to protect Plaintiffs; and

k. for purchasers' of Equifax's own credit monitoring and identity theft protection products, diminution of the value and/or loss of the benefits of those products.

COUNT 3

NEGLIGENCE *PER SE*

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

348. Plaintiffs repeat and reallege Paragraphs 1-313, as if fully alleged herein.

349. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the Federal Trade Commission ("FTC"), the unfair act or practice by companies such as Equifax of failing to use reasonable measures to protect Personal Information. Various FTC publications and orders also form the basis of Equifax's duty.

350. Equifax violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Personal Information and not complying with industry standards. Equifax's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained and stored and the foreseeable consequences of a data breach at one of the three major credit bureaus.

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

352. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) was intended to protect.

353. Moreover, 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 harm suffered by Plaintiffs and the Class.

354. As a direct and proximate result of Equifax's negligence, Plaintiffs and Class members have been injured as described herein and in Paragraph 347 above, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

COUNT 4

GEORGIA FAIR BUSINESS PRACTICES ACT

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Georgia Subclass

355. Plaintiffs repeat and allege Paragraphs 1-313, as if fully alleged herein.

356. Equifax, Plaintiffs, and Class members are "persons" within the meaning of the Georgia Fair Business Practices Act ("GFBPA"). O.C.G.A. § 10-1-399(a).

357. Equifax is engaged in, and its acts and omissions affect, trade and commerce under O.C.G.A. § 10-1-392(28). Further, Equifax is engaged in "consumer acts or practices," which are defined as "acts or practices intended to encourage consumer transactions" under O.C.G.A. § 10-1-392(7). Equifax, in its capacity as a "consumer reporting agency," generates and maintains "consumer reports" and "files" subject to the GFBPA. O.C.G.A. §10-1-392 (9)-(10), (14).

358. Equifax's acts, practices, and omissions at issue in this matter were directed and emanated from its headquarters in Georgia.

359. Equifax engaged in "[u]nfair or deceptive acts or practices in the conduct of consumer transactions and consumer acts or practices in trade or commerce" in violation of O.C.G.A. § 10-1-393(a). Those acts and practices include those expressly declared unlawful by O.C.G.A. § 10-1-393(b), such as:

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. Advertising goods or services with intent not to sell them as advertised.

360. In addition, Equifax engaged in the unfair and deceptive acts and practices described below that, while not expressly declared unlawful by O.C.G.A. § 10-1-393(b), are prohibited by O.C.G.A. § 10-1-393(a).

361. In the course of its business, Equifax engaged in unfair acts and practices prohibited by O.C.G.A. § 10-1-393(a), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Class members' Personal Information, which was a direct and proximate cause of the Equifax data breach and its immense scope;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, adequately improve security and privacy measures following previous cybersecurity incidents, and detect and redress the Equifax data breach while it was ongoing, which were a direct and proximate cause of the Equifax data breach and its immense scope; and

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Class members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*, which was a direct and proximate cause of the Equifax data breach and its immense scope.

362. In the course of its business, Equifax also engaged in deceptive acts and practices prohibited by O.C.G.A. § 10-1-393(a), including:

a. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class members' Personal Information, including by implementing and maintaining reasonable security measures;

b. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

c. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' Personal Information; and

d. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security of Plaintiffs and Class members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

363. The misrepresentations and omissions described in the preceding paragraph were material and made intentionally and knowingly with the intent that Plaintiffs, Class members, and others (such as its customers, data furnishers, regulators, investors, participants in the credit markets, and those who otherwise used data from Equifax for business purposes) rely upon them in connection with accessing and storing the extremely sensitive and valuable Personal Information of Plaintiffs and Class members.

364. Equifax did all of this directly with respect to Plaintiffs and Class members, and also by way of their transactions involving goods, merchandise, and services with third parties (such as prospective creditors and creditors) who also

accessed Plaintiffs' and Class members' sensitive and valuable Personal Information in the course of those transactions.

365. For years, Equifax knew of the inadequate security controls and vulnerabilities in its data security systems and the key databases storing Plaintiff and the Class members' sensitive and valuable Personal Information, but concealed all of these security failings.

366. Equifax's deceptive acts and practices were likely to and did in fact deceive the public at large and reasonable consumers, including Plaintiffs and Class members, regarding the security and safety of the Personal Information in its care, including the Personal Information of Plaintiffs and Class members. Equifax's deceptive acts and practices also were intended to and did in fact deceive others who relied upon Equifax to maintain the security of the Personal Information in its care, including its customers, data furnishers, regulators, investors, participants in the credit markets, and others who used data from Equifax for business purposes.

367. Equifax's representations and omissions were material to Plaintiffs, Class members, and others (such as Equifax's customers, data furnishers, regulators, investors, participants in the credit markets, and those who used data from Equifax for business purposes) given the extreme sensitivity, value, and

importance of the Personal Information maintained by Equifax; the uncertainty and disruption that would inevitably occur if the marketplace were informed Equifax did not adequately protect Personal Information; and the obvious adverse consequences to participants in the American economy from a substantial data breach at Equifax.

368. Equifax knew or should have known that by collecting, selling, and trafficking in Personal Information, Plaintiffs, Class members, and others (such as Equifax's customers, data furnishers, regulators, investors, participants in the credit markets, and those who used data from Equifax for business purposes) would reasonably rely upon and assume Equifax's data systems were secure unless Equifax otherwise informed them.

369. Because Equifax's primary product was the sale and analysis of highly sensitive Personal Information, and because Equifax controlled the compilation of and access to such Personal Information, Plaintiffs, Class members, and others involved (such as Equifax's customers, data furnishers, regulators, investors, participants in the credit markets, and those who used data from Equifax for business purposes) relied upon Equifax to advise if its data systems were not secure and, thus, Personal Information could be compromised.

370. Plaintiffs, Class members, and others who relied upon Equifax to maintain adequate data security systems had no effective means on their own to discover the truth. In particular, Equifax did not afford Plaintiffs and Class members any opportunity to inspect Equifax's data security, learn that it was inadequate and non-compliant with legal requirements, or otherwise ascertain the truthfulness of Equifax's representations and omissions regarding Equifax's ability to protect data and comply with the law.

371. Plaintiffs, Class members, and others (such as Equifax's customers, data furnishers, regulators, investors, participants in the credit markets, and those who used data from Equifax for business purposes) relied to their detriment upon Equifax's representations and omissions regarding data security, including Equifax's failure to alert customers that its privacy and security protections were inadequate and insecure and thus were vulnerable to attack.

372. Had Equifax disclosed to Plaintiffs, Class members, and others (such as Equifax's customers, data furnishers, regulators, investors, participants in the credit markets, and those who used data from Equifax for business purposes) 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 serve as trusted linchpins of the financial system and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers. Equifax accepted the responsibility of being a "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, Plaintiffs, Class members, and others acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

373. Equifax acted intentionally, knowingly, and maliciously to violate the GFBPA, and recklessly disregarded Plaintiffs and Class members' rights.

374. Equifax's violations present a continuing risk to Plaintiffs and Class members, as well as to the general public.

375. Equifax's unlawful acts and practices complained of herein affect the consumer marketplace and the public interest, including the 147.9 million U.S residents and 5.3 million Georgians affected by the Equifax data breach.

376. But for Equifax's violations of the GFBPA described above, the Equifax data breach would not have occurred.

377. As a direct and proximate result of Equifax's violations of the GFBPA, Plaintiffs and Class members have suffered injury-in-fact, monetary, and non-monetary damages, including damages from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information, and/or actual damages, as described herein.

378. The GFBPA permits any person who suffers injury or damages as a result of the violation of its provisions to bring an action against the person or persons engaged in such violations. O.C.G.A. § 10-1-399(a).

379. Pursuant to O.C.G.A. § 10-1-399(b), at least 30 days prior to bringing this claim, Plaintiffs provided Equifax with a written demand for relief describing the unfair or deceptive act or practice relied upon and the injury suffered by them. More than 30 days have elapsed since the service of that written demand. No written tender of settlement has been made by Equifax.

380. Plaintiffs bring this action on behalf of themselves and Class members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers and the public at large to make informed decisions related to the security of their sensitive Personal Information, and to protect the public from Equifax's unfair

methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices.

381. Plaintiffs and Class members are entitled to a judgment against Equifax for actual and consequential damages; general, nominal, exemplary, and trebled damages and attorneys' fees pursuant to the GFBPA; costs; and such other further relief as the Court deems just and proper.

COUNT 5

UNJUST ENRICHMENT

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

382. Plaintiffs repeat and reallege Paragraphs 1-313, as if fully alleged herein.

383. Plaintiffs and Class members have an interest, both equitable and legal, in the Personal Information about them that was conferred upon, collected by, and maintained by Equifax and that was ultimately stolen in the Equifax data breach. This Personal Information was conferred on Equifax in most cases by third-parties but in some instances directly by Plaintiffs and Class members themselves.

384. Equifax was benefitted by the conferral upon it of the Personal Information pertaining to Plaintiffs and Class members and by its ability to retain and use that information. Equifax understood that it was in fact so benefitted.

385. Equifax also understood and appreciated that the Personal Information pertaining to Plaintiffs and Class members was private and confidential and its value depended upon Equifax maintaining the privacy and confidentiality of that Personal Information.

386. But for Equifax's willingness and commitment to maintain its privacy and confidentiality, that Personal Information would not have been transferred to and entrusted with Equifax. Further, if Equifax had disclosed that its data security measures were inadequate, Equifax would not have been permitted to continue in operation by regulators, its shareholders, and participants in the marketplace.

387. As a result of Equifax's wrongful conduct as alleged in this Complaint (including among things its utter failure to employ adequate data security measures, its continued maintenance and use of the Personal Information belonging to Plaintiffs and Class members without having adequate data security measures, and its other conduct facilitating the theft of that Personal Information), Equifax has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Class members. Among other things, Equifax continues to benefit

and profit from the sale of the Personal Information while its value to Plaintiffs and Class members has been diminished.

388. Equifax's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and Class members' sensitive Personal Information, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

389. Under the common law doctrine of unjust enrichment, it is inequitable for Equifax to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiffs and Class members in an unfair and unconscionable manner. Equifax's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

390. The benefit conferred upon, received, and enjoyed by Equifax was not conferred officiously or gratuitously, and it would be inequitable and unjust for Equifax to retain the benefit.

391. Equifax is therefore liable to Plaintiffs and Class members for restitution in the amount of the benefit conferred on Equifax as a result of its wrongful conduct, including specifically the value to Equifax of the Personal

Information that was stolen in the Equifax data breach and the profits Equifax is receiving from the use and sale of that information.

COUNT 6

DECLARATORY JUDGMENT

On Behalf of Plaintiffs and the Nationwide Class, or Alternatively, on Behalf of Plaintiffs and the Statewide Subclasses

392. Plaintiffs repeat and allege Paragraphs 1-313, as if fully alleged herein.

393. 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 violate the terms of the federal and state statutes described in this Complaint.

394. An actual controversy has arisen in the wake of the Equifax data breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Personal Information and whether Equifax is currently maintaining data security measures adequate to protect Plaintiffs and Class members from further data breaches that compromise their Personal Information. Plaintiffs allege that Equifax's data security measures remain inadequate. Equifax denies these allegations. Furthermore, Plaintiffs continue to

suffer injury as a result of the compromise of their Personal Information and remain at imminent risk that further compromises of their Personal Information will occur in the future.

395. 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 secure consumers' Personal Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes;

b. Equifax continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Personal Information.

396. The Court also should issue corresponding prospective injunctive relief requiring Equifax to employ adequate security protocols consistent with law and industry standards to protect consumers' Personal Information.

397. 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. 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.

398. The hardship to Plaintiffs 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, Plaintiffs will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to Equifax of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Equifax has a pre-existing legal obligation to employ such measures.

399. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Equifax, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose confidential information would be further compromised.

CLAIMS ON BEHALF OF THE EQUIFAX CONTRACT SUBCLASS

COUNT 7

BREACH OF CONTRACT

On Behalf of Plaintiffs and the Nationwide Equifax Contract Subclass, or alternatively, On Behalf of Plaintiffs and Each of the Equifax Contract Statewide Subclasses

400. Plaintiffs Christy Adams, Michael Bishop, Ricardo Clemente, Thomas Cromwell, Germany Davis, Christopher Dunleavy, Robert Etten, Michael Getz, Tabitha Thomas Hawkins, Alexander Hepburn, Kathleen Holly, Michael Hornblas, Alvin Kleveno, Jr., Maria Martucci, Anthony Mirarchi, Sanjay Rajput, David Sands, Maria Schifano, and Richard Whittington II ("Plaintiffs," for purposes of this Count) repeat and allege Paragraphs 1-313, as if fully alleged herein.

401. Equifax's Privacy Policy is an agreement between Equifax and individuals who provided their personal information to Equifax, including Plaintiffs and Class members.

402. Equifax's Privacy Policy states, among other things, that Equifax "restrict[s] access to personally identifiable information . . . that is collected about you to only those who have a need to know that information in connection with the purpose for which it is collected and used."

403. Equifax agreed 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 agreed that "we have security protocols and measures in place to protect the personally identifiable information . . . and other information we maintain 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."

404. Equifax emphasized its "commitment" to "protect the privacy and confidentiality of personal information about consumers, and agreed that "[s]afeguarding the privacy and security of information, both online and offline, is a top priority for Equifax."

405. Plaintiffs and Class members on the one side and Equifax on the other formed a contract when Plaintiffs and Class members obtained credit monitoring or identity theft protection services from Equifax, or otherwise provided Personal Information to Equifax subject to its Privacy Policy (through obtaining disclosures of their credit files, disputing items in their credit files, or taking action associated with a fraud alert, active duty alert, or security freeze or lock on their credit files).

406. Plaintiffs and Class members fully performed their obligations under the contracts with Equifax.

407. Equifax breached its agreement with Plaintiffs and Class members by failing to protect their Personal Information. Specifically, it (1) failed to take reasonable steps to use safe and secure systems to protect that information; (2) failed to have appropriate security protocols and measures in place to protect that information, such as adequate internal and external firewalls, physical security, technological security measures, and encryption; (3) disclosed that information to unauthorized third parties; and (4) failed to promptly alert or give notice of the breach to Plaintiffs and Class members.

408. As a direct and proximate result of Equifax's breaches of contract, Plaintiffs and Class members sustained actual losses and damages as described in detail above, and are also entitled to recover nominal damages.

COUNT 8

BREACH OF IMPLIED CONTRACT

On Behalf of Plaintiffs and the Nationwide Equifax Contract Subclass, or alternatively, On Behalf of Plaintiffs and Each of the Equifax Contract Statewide Subclasses

409. Plaintiffs Christy Adams, Michael Bishop, Ricardo Clemente, Thomas Cromwell, Germany Davis, Christopher Dunleavy, Robert Etten, Michael Getz,

Tabitha Thomas Hawkins, Alexander Hepburn, Kathleen Holly, Michael Hornblas, Alvin Kleveno, Jr., Maria Martucci, Anthony Mirarchi, Sanjay Rajput, David Sands, Maria Schifano, and Richard Whittington II ("Plaintiffs," for purposes of this Count) repeat and allege Paragraphs 1-313, as if fully alleged herein.

410. Plaintiffs and Class members entered into an implied contract with Equifax when they obtained credit monitoring or identity theft protection services from Equifax, or otherwise provided Personal Information to Equifax subject to its Privacy Policy (through obtaining disclosures of their credit files, disputing items in their credit files, or taking action associated with a fraud alert, active duty alert, or security freeze or lock on their credit files).

411. As part of these transactions, Equifax agreed to safeguard and protect the Personal Information of Plaintiffs and Class members and to timely and accurately notify them if their Personal Information was breached or compromised.

412. Plaintiffs and Class members entered into the implied contracts with the reasonable expectation that Equifax's data security practices and policies were reasonable and consistent with industry standards. Plaintiffs and Class members believed that Equifax would use part of the monies paid to Equifax under the implied contracts to fund adequate and reasonable data security practices.

413. Plaintiffs and Class members would not have obtained Equifax's credit monitoring or identity theft protection services or provided and entrusted their Personal Information to Equifax, in the absence of the implied contract or implied terms between them and Equifax. The safeguarding of the Personal Information of Plaintiffs and Class members and prompt and sufficient notification of a breach was critical to realize the intent of the parties.

414. Plaintiffs and Class members fully performed their obligations under the implied contracts with Equifax.

415. Equifax breached its implied contracts with Plaintiffs and Class members to protect their Personal Information when it (1) failed to have security protocols and measures in place to protect that information; (2) disclosed that information to unauthorized third parties; and (3) failed to provide timely and accurate notice that their Personal Information was compromised as a result of the data breach.

416. As a direct and proximate result of Equifax's breaches of implied contract, Plaintiffs and Class members sustained actual losses and damages as described in detail above, and are also entitled to recover nominal damages.

CLAIMS ON BEHALF OF THE FCRA DISCLOSURE SUBCLASS

COUNT 9

VIOLATION OF THE FAIR CREDIT REPORTING ACT, 15 U.S.C. § 1681g(a)

On Behalf of the FCRA Disclosure Subclass

417. Plaintiffs Grace Cho and Debra Lee repeat and allege Paragraphs 1-313, as if fully alleged herein, including specifically Paragraphs 109-121.

418. Plaintiffs and FCRA Disclosure Subclass members requested and obtained from Equifax disclosures governed by 15 U.S.C. § 1681g after Equifax learned of the Equifax data breach.

419. These disclosures failed to clearly and accurately disclose all information in these consumers' files at the time of the request, including the existence of the breach and the existence or identity of each person that procured a consumer report.

420. Equifax's failure to clearly and accurately disclose the fraudulent procurement of this credit information, and to identify, either specifically or in general terms, the person who procured a consumer report through the Equifax data breach, violated section 1681g(a)(1) and (3) of the FCRA.

421. Plaintiffs and Class members suffered actual injury because of Equifax's violations of section 1681g(a)(1) and (3) of the FCRA. They purchased

or received by entitlement a valuable consumer disclosure, which was less valuable because Plaintiffs and Class members were denied important information that was to have been part of their consumer disclosure otherwise to be provided upon request. They also were deprived of their opportunity to meaningfully consider and address issues relating to potential identity theft and fraud, as well as to avail themselves of the procedures and remedies available under sections 1681c-1 and 1681c-2 of the FCRA.

422. Because the consumer disclosures Equifax provided after it learned of the breach did not include all of the information Equifax was obligated to include in those consumer disclosures, they were worth some amount less.

423. Additionally, the rights at issue were determined by Congress to be important measures of Equifax's process to ensure continued accuracy and completeness in its files and reports.

424. The conduct, action, and inaction of Equifax was willful, rendering Equifax liable for statutory and punitive damages in an amount to be determined pursuant to 15 U.S.C. § 1681n.

425. Plaintiffs and members of the FCRA Disclosure Subclass are entitled to recover costs and attorneys' fees, as well as appropriate equitable relief, from Equifax, in an amount to be determined pursuant to 15 U.S.C. § 1681n.

426. Therefore, Equifax is liable to Plaintiffs and Class members in an amount equal to actual damages, or damages of not less than $100 and not more than $1,000 for each Plaintiff and Class member, as well as punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a).

427. In the alternative, Equifax's violations were negligent, entitling Plaintiffs and Class members to costs, attorneys' fees, and actual damages, in an amount to be determined at trial.

CLAIMS ON BEHALF OF THE ALABAMA SUBCLASS

COUNT 10

ALABAMA DECEPTIVE TRADE PRACTICES ACT, Ala. Code §§ 8-19-1, *et seq.*

428. The Alabama Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Alabama Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

429. Equifax is a "person" as defined by Ala. Code § 8-19-3(5).

430. Plaintiff and Alabama Subclass members are "consumers" as defined by Ala. Code § 8-19-3(2).

431. Plaintiff sent pre-suit notice pursuant to Ala. Code § 8-19-10(e) on October 10, 2017.

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

433. Equifax engaged in deceptive acts and practices in the conduct of trade or commerce, in violation of the Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-5, including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have;

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

c. Engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce, including acts and practices that would violate Section 5(a)(1) of the FTC Act, as interpreted by the FTC and federal courts.

434. Equifax's deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Alabama Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Alabama Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and Alabama Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Alabama Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Alabama Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Alabama Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

435. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

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

437. 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 serve as trusted linchpins of the financial system and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Alabama Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the Alabama Subclass members acted

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

438. Equifax acted intentionally, knowingly, and maliciously to violate the Alabama Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Alabama Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

439. As a direct and proximate result of Equifax's deceptive acts and practices, Plaintiff and Alabama Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

440. Equifax's deceptive acts and practices caused substantial injury to Plaintiff and Alabama Subclass members, which they could not reasonably avoid, and which outweighed any benefits to consumers or to competition.

441. Plaintiff and the Alabama Subclass seek all monetary and non-monetary relief allowed by law, including the greater of (a) actual damages or (b)

statutory damages of $100; treble damages; injunctive relief; attorneys' fees, costs, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE ALASKA SUBCLASS

COUNT 11

PERSONAL INFORMATION PROTECTION ACT, Alaska Stat. §§ 45.48.010, *et seq.*

442. The Alaska Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Alaska Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

443. Equifax is a business that owns or licenses Personal Information as defined by Alaska Stat. § 45.48.090(7). As such a business, it is a Covered Person as defined in Alaska Stat. § 45.48.010(a).

444. Plaintiff and Alaska Subclass members' Personal Information (*e.g.*, Social Security numbers) includes Personal Information as covered under Alaska Stat. § 45.48.010(a).

445. Equifax is required to accurately notify Plaintiff and Alaska Subclass members if it becomes aware of a breach of its data security system in the most expeditious time possible and without unreasonable delay under Alaska Stat. § 45.48.010(b).

446. Equifax is similarly required to determine the scope of the breach and restore the reasonable integrity of the information system under Alaska Stat. § 45.48.010(b).

447. Because Equifax was aware of a breach of its security system, Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Alaska Stat. § 45.48.010(b).

448. By failing to disclose the Equifax data breach in a timely and accurate manner Equifax violated Alaska Stat. § 45.48.010(b).

449. Pursuant to Alaska Stat. § 45.48.080(b), a violation of Alaska Stat. § 45.48.010(b) is an unfair or deceptive act or practice under the Alaska Consumer Protection Act.

450. As a direct and proximate result of Equifax's violations of Alaska Stat. § 45.48.010(b), Plaintiff and Alaska Subclass members suffered damages, as described above.

451. Plaintiff and Alaska Subclass members seek relief measured as the greater of (a) each unlawful act, (b) three times actual damages in an amount to be determined at trial, or (c) statutory damages in the amount of $500 for Plaintiff and each Alaska Subclass Member; reasonable attorneys' fees; and any other just and

proper relief available under Alaska Stat. § 45.48.080(b)(2) and Alaska Stat. § 45.50.531.

COUNT 12

ALASKA CONSUMER PROTECTION ACT, Alaska Stat. §§ 45.50.471, *et seq.*

452. The Alaska Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Alaska Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

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

454. Alaska Subclass members are "consumers" as defined by Alaska Stat. § 45.50.561(4).

455. Equifax engaged in unfair or deceptive acts and practices in the conduct of trade or commerce, in violation Alaska Stat. § 45.50.471, including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or qualities that they do not have;

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

c. Advertising goods or services with intent not to sell them as advertised;

d. Engaging in any other conduct creating a likelihood of confusion or of misunderstanding and which misleads, deceives, or damages a buyer in connection with the sale or advertisements of its goods or services; and

e. Using or employing deception, fraud, false pretense, false promise, misrepresentation, or knowingly concealing, suppressing, or omitting a material fact with intent that others rely upon the concealment, suppression, or omission in connection with the sale or advertisement of its goods or services whether or not a person was in fact misled, deceived, or damaged.

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

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Alaska Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Alaska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and Alaska Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Alaska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the

FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Alaska Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Alaska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

457. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

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

459. Equifax acted intentionally, knowingly, and maliciously to violate Alaska's Consumer Protection Act, and recklessly disregarded Plaintiff and Alaska

Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

460. As a direct and proximate result of Equifax's unfair and deceptive acts and practices, Plaintiff and Alaska Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

461. Plaintiff and the Alaska Subclass seek all monetary and non-monetary relief allowed by law, including the greater of (a) three times their actual damages or (b) statutory damages in the amount of $500; punitive damages; reasonable attorneys' fees and costs; injunctive relief; and any other relief that is necessary and proper.

CLAIMS ON BEHALF OF THE ARIZONA SUBCLASS

COUNT 13

ARIZONA CONSUMER FRAUD ACT, A.R.S. §§ 44-1521, *et seq.*

462. The Arizona Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Arizona Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

463. Equifax is a "person" as defined by A.R.S. § 44-1521(6).

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

465. Equifax engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment, suppression, and omission of material facts affecting the people of Arizona in connection with the sale and advertisement of "merchandise" (as defined in Arizona Consumer Fraud Act, A.R.S. § 44-1521(5)) in violation of A.R.S. § 44-1522(A), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Arizona Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arizona Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and Arizona Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arizona Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the

FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Arizona Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arizona Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

466. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

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

468. 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 serve as trusted linchpins of the financial system and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Arizona Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the Arizona Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

469. Equifax acted intentionally, knowingly, and maliciously to violate Arizona's Consumer Fraud Act, and recklessly disregarded Plaintiff and Arizona Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

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

and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

471. Plaintiff and Arizona Subclass members seek all monetary and non-monetary relief allowed by law, including compensatory damages; disgorgement; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE ARKANSAS SUBCLASS

COUNT 14

ARKANSAS DECEPTIVE TRADE PRACTICES ACT, A.C.A. §§ 4-88-101, *et seq.*

472. The Arkansas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Arkansas Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

473. Equifax is a "person" as defined by A.C.A. § 4-88-102(5).

474. Equifax's products and services are "goods" and "services" as defined by A.C.A. §§ 4-88-102(4) and (7).

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

476. The Arkansas Deceptive Trade Practices Act ("ADTPA"), A.C.A. §§ 4-88-101, *et seq.*, prohibits unfair, deceptive, false, and unconscionable trade practices.

477. Equifax engaged in acts of deception and false pretense in connection with the sale and advertisement of services in violation of A.C.A. § 4-88-1-8(1) and concealment, suppression and omission of material facts, with intent that others rely upon the concealment, suppression or omission in violation of A.C.A. § 4-88-1-8(2), and engaged in the following deceptive and unconscionable trade practices defined in A.C.A. § 4-88-107:

a. Knowingly making a false representation as to the characteristics, ingredients, uses, benefits, alterations, source, sponsorship, approval, or certification of goods or services and as to goods being of a particular standard, quality, grade, style, or model;

b. Advertising goods or services with the intent not to sell them as advertised;

c. Employing consistent bait-and-switch advertising of an attractive but insincere offer to sell a product or service which the seller in truth does not intend or desire to sell, as evidenced

by acts demonstrating an intent not to sell the advertised product or services;

d. Knowingly taking advantage of a consumer who is reasonably unable to protect his or her interest because of ignorance; and

e. Engaging in other unconscionable, false, or deceptive acts and practices in business, commerce, or trade.

478. Equifax's unconscionable, false, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Arkansas Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arkansas

Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and the Arkansas Personal Information Protection Act, A.C.A. § 4-110-104(b), which was a direct and proximate cause of the Equifax data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Arkansas Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arkansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and the Arkansas Personal Information Protection Act, A.C.A. § 4-110-104(b);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Arkansas Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Arkansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and the Arkansas Personal Information Protection Act, A.C.A. § 4-110-104(b).

479. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

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

481. 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 serve as trusted linchpins of the financial system and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Arkansas Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the Arkansas Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

482. Equifax acted intentionally, knowingly, and maliciously to violate Arkansas's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Arkansas Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

483. As a direct and proximate result of Equifax's unconscionable, unfair, and deceptive acts or practices and Plaintiff and Arkansas Subclass members' reliance thereon, Plaintiff and Arkansas Subclass members have suffered and will

continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

484. Plaintiff and the Arkansas Subclass members seek all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT 15

CALIFORNIA CUSTOMER RECORDS ACT, Cal. Civ. Code §§ 1798.80, *et seq.*

485. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

486. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the

Personal Information from unauthorized access, destruction, use, modification, or disclosure."

487. Equifax is a business that owns, maintains, and licenses Personal Information, within the meaning of Cal. Civ. Code § 1798.81.5, about Plaintiff and California Subclass members.

488. Businesses that own or license computerized data that includes Personal Information, including Social Security numbers, are required to notify California residents when their Personal Information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

489. Equifax is a business that owns or licenses computerized data that includes Personal Information as defined by Cal. Civ. Code § 1798.82.

490. Plaintiff and California Subclass members' Personal Information (*e.g.*, Social Security numbers) includes Personal Information as covered by Cal. Civ. Code § 1798.82.

491. Because Equifax reasonably believed that Plaintiff's and California Subclass members' Personal Information was acquired by unauthorized persons during the Equifax data breach, Equifax had an obligation to disclose the Equifax data breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

492. By failing to disclose the Equifax data breach in a timely and accurate manner, Equifax violated Cal. Civ. Code § 1798.82.

493. As a direct and proximate result of Equifax's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and California Subclass members suffered damages, as described above.

494. Plaintiff and California Subclass members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT 16

CALIFORNIA UNFAIR COMPETITION LAW, Cal. Bus. & Prof. Code §§ 17200, *et seq.*

495. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

496. Equifax is a "person" as defined by Cal. Bus. & Prof. Code §17201.

497. Equifax violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

498. Equifax's "unfair" acts and practices include:

a. Equifax failed to implement and maintain reasonable security measures to protect Plaintiff and California Subclass members' Personal Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Equifax data breach. Equifax failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents. For example, Equifax failed to patch the well-known Apache Struts vulnerability, which made it trivial for a hacker to penetrate Equifax's systems. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and the California Subclass, whose Personal Information has been compromised.

b. Equifax's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), the Gramm-Leach Bliley Act (15 U.S.C. § 6801(a)), and California's Consumer Records Act (Cal. Civ. Code § 1798.81.5).

c. Equifax's failure to implement and maintain reasonable security measures also lead to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Equifax's inadequate security, consumers could not have reasonably avoided the harms that Equifax caused.

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

499. Equifax has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§

1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq.*, the FCRA, 15 U.S.C. §§ 1681e (alleged above), the GLBA, 15 U.S.C. § 680, *et seq.*, the FTC Act, 15 U.S.C. § 45, and California common law.

500. Equifax's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and California Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and California's

Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*, which was a direct and proximate cause of the Equifax data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and California Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and California Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties

pertaining to the security and privacy of Plaintiff and California Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq.*

501. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

502. As a direct and proximate result of Equifax's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California Subclass members were injured and lost money or property, including the costs passed through to Equifax from their consumer credit transactions, the premiums and/or price received by Equifax for its goods and services, monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Personal Information.

503. Equifax acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff and

California Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

504. Plaintiff and California Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from Equifax's unfair, unlawful, and fraudulent business practices or use of their Personal Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT 17

CALIFORNIA CONSUMER LEGAL REMEDIES ACT, Cal. Civ. Code §§ 1750, *et seq.*

505. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

506. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses providing goods, property or services to consumers primarily for personal, family, or household use.

507. Equifax is a "person" as defined by Civil Code §§ 1761(c) and 1770, and has provided "services" as defined by Civil Code §§ 1761(b) and 1770.

508. Plaintiff and the California Class are "consumers" as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

509. Equifax's acts and practices were intended to and did result in the sales of products and services to Plaintiff and the California Subclass members in violation of Civil Code § 1770, 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 when they were not;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

510. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data

security and ability to protect the confidentiality of consumers' Personal Information.

511. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the California Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the California Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

512. As a direct and proximate result of Equifax's violations of California Civil Code § 1770, Plaintiff and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and

monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

513. Plaintiff and the California Subclass have provided notice of their claims for damages to Equifax, in compliance with California Civil Code § 1782(a).

514. Plaintiff and the California Subclass seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

CLAIMS ON BEHALF OF THE COLORADO SUBLCASS

COUNT 18

COLORADO SECURITY BREACH NOTIFICATION ACT, Colo. Rev. Stat. §§ 6-1-716, *et seq.*

515. The Colorado Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Colorado Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

516. Equifax is a business that owns or licenses computerized data that includes Personal Information as defined by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

517. Plaintiff and Colorado Subclass members' Personal Information (*e.g.*, Social Security numbers) includes Personal Information as covered by Colo. Rev. Stat. §§ 6-1-716(1) and 6-1-716(2).

518. Equifax is required to accurately notify Plaintiff and Colorado Subclass members if it becomes aware of a breach of its data security system in the most expedient time possible and without unreasonable delay under Colo. Rev. Stat. § 6-1-716(2).

519. Because Equifax was aware of a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Colo. Rev. Stat. § 6-1-716(2).

520. By failing to disclose the Equifax data breach in a timely and accurate manner, Equifax violated Colo. Rev. Stat. § 6-1-716(2).

521. As a direct and proximate result of Equifax's violations of Colo. Rev. Stat. § 6-1-716(2), Plaintiff and Colorado Subclass members suffered damages, as described above.

522. Plaintiff and Colorado Subclass members seek relief under Colo. Rev. Stat. § 6-1-716(4), including actual damages and equitable relief.

COUNT 19

COLORADO CONSUMER PROTECTION ACT, Colo. Rev. Stat. §§ 6-1-101, *et seq.*

523. The Colorado Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Colorado Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

524. Equifax is a "person" as defined by Colo. Rev. Stat. § 6-1-102(6).

525. Equifax engaged in "sales" as defined by Colo. Rev. Stat. § 6-1-102(10).

526. Plaintiff and Colorado Subclass members, as well as the general public, are actual or potential consumers of the products and services offered by Equifax or successors in interest to actual consumers.

527. Equifax engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. § 6-1-105(1), including:

a. Knowingly making a false representation as to the characteristics of products and services;

b. Representing that services are of a particular standard, quality, or grade, though Equifax knew or should have known that there were or another;

c. Advertising services with intent not to sell them as advertised; and

d. Failing to disclose material information concerning its services which was known at the time of an advertisement or sale when the failure to disclose the information was intended to induce the consumer to enter into the transaction.

528. Equifax's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Colorado Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Colorado Subclass members' Personal Information, including duties

imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and Colorado Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Colorado Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Colorado Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Colorado

Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

529. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

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

531. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Colorado Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the Colorado Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

532. Equifax acted intentionally, knowingly, and maliciously to violate Colorado's Consumer Protection Act, and recklessly disregarded Plaintiff and Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

533. As a direct and proximate result of Equifax's deceptive trade practices, Colorado Subclass members suffered injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their personal information.

534. Equifax's deceptive trade practices significantly impact the public, because nearly all members of the public are actual or potential consumers of Equifax's services and the Equifax data breach affected more than 147 million Americans, including 2.5 million Coloradans.

535. Plaintiff and Colorado Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of: (a) actual damages, or (b)

$500, or (c) three times actual damages (for Equifax's bad faith conduct); injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE CONNECTICUT SUBCLASS

COUNT 20

BREACH OF SECURITY REGARDING COMPUTERIZED DATA, C.G.S.A. § 36a-701b

536. The Connecticut Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Connecticut Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

537. Equifax is a business that conducts business in Connecticut and owns, licenses, and maintains computerized data that includes personal information as covered by C.G.S.A. § 36a-701b(b). Equifax also maintains computerized data that includes personal information that it does not own as covered by C.G.S.A. § 36a-701b(c).

538. Plaintiff and Connecticut Subclass members' Personal Information (*e.g.*, Social Security numbers) includes Personal Information as covered by C.G.S.A. § 36a-701b(a).

539. Equifax is required to accurately notify Plaintiff and Connecticut Subclass members if it becomes aware of a breach of its data security system in the

most expedient time possible and without unreasonable delay, not to exceed ninety days after discovery of the breach under C.G.S.A. § 36a-701b(b).

540. Equifax is required to immediately notify Plaintiff and Connecticut Subclass members if it becomes aware of a breach of its data security system which may have compromised personal information Equifax stores but Plaintiff and Connecticut Class members own under C.G.S.A. § 36a-701b(c).

541. Because Equifax was aware of a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by C.G.S.A. §§ 36a-701b(b) and (c).

542. By failing to disclose the Equifax data breach in an accurate and timely manner, Equifax failed to comply with C.G.S.A. §§ 36a-701b(b) and (c). Pursuant to C.G.S.A. § 36a-701b(g), Equifax's failure to comply was an unfair trade practice under the Connecticut Unfair Trade Practices Act, C.G.S.A. §§ 42-110a, *et seq.*

543. As a direct and proximate result of Equifax's violations of C.G.S.A. §§ 36a-701b(b) and (c), Plaintiff and Connecticut Subclass members suffered damages, as described above.

544. Plaintiff and Connecticut Subclass members seek relief under C.G.S.A. § 42-110g for the harm they suffered because of Equifax's violations of C.G.S.A. §§ 36a-701b(b) and (c), including actual damages and equitable relief.

CLAIMS ON BEHALF OF THE DELAWARE SUBCLASS

COUNT 21

DELAWARE COMPUTER SECURITY BREACH ACT, 6 Del. Code Ann. §§ 12B-102, *et seq.*

545. The Delaware Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Delaware Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

546. Equifax is a business that owns or licenses computerized data that includes Personal Information as defined by 6 Del. Code Ann. § 12B-102(a).

547. Plaintiff and Delaware Subclass members' Personal Information (*e.g.*, Social Security numbers) includes Personal Information as covered under 6 Del. Code Ann. § 12B-101(4).

548. Equifax is required to accurately notify Plaintiff and Delaware Subclass members if Equifax becomes aware of a breach of its data security system which is reasonably likely to result in the misuse of a Delaware resident's Personal Information, in the most expedient time possible and without unreasonable delay under 6 Del. Code Ann. § 12B-102(a).

549. Because Equifax was aware of a breach of its security system which is reasonably likely to result in misuse of Delaware residents' Personal Information, Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by 6 Del. Code Ann. § 12B-102(a).

550. By failing to disclose the Equifax data breach in a timely and accurate manner, Equifax violated 6 Del. Code Ann. § 12B-102(a).

551. As a direct and proximate result of Equifax's violations of 6 Del. Code Ann. § 12B-102(a), Plaintiff and Delaware Subclass members suffered damages, as described above.

552. Plaintiff and Delaware Subclass members seek relief under 6 Del. Code Ann. § 12B-104, including actual damages and equitable relief.

COUNT 22

DELAWARE CONSUMER FRAUD ACT, 6 Del. Code §§ 2513, *et seq.*

553. The Delaware Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Delaware Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

554. Equifax is a "person" that is involved in the "sale" of "merchandise," as defined by 6 Del. Code § 2511(7), (8), and (6).

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

556. Equifax used and employed deception, fraud, false pretense, false promise, misrepresentation, and the concealment, suppression, and omission of material facts with intent that others rely upon such concealment, suppression and omission, in connection with the sale and advertisement of merchandise, in violation of 6 Del. Code § 2513(a), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Delaware Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Delaware Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Delaware's data security statute, 6 Del. Code § 12B-100, which was a direct and proximate cause of the Equifax data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Delaware Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Delaware Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Delaware's data security statute, 6 Del. Code § 12B-100;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Delaware Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Delaware Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Delaware's data security statute, 6 Del. Code § 12B-100.

557. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

558. Equifax acted intentionally, knowingly, and maliciously to violate Delaware's Consumer Fraud Act, and recklessly disregarded Plaintiff and Delaware Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

559. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Delaware Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the Delaware Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

560. Equifax's unlawful trade practices were gross, oppressive, and aggravated, and Equifax breached the trust of Plaintiff and the Delaware Subclass members.

561. As a direct and proximate result of Equifax's unlawful acts and practices, Plaintiff and Delaware Subclass members have suffered and will

continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

562. Plaintiff and Delaware Subclass members seek all monetary and non-monetary relief allowed by law, including damages under 6 Del. Code § 2525 for injury resulting from the direct and natural consequences of Equifax's unlawful conduct; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE DISTRICT OF COLUMBIA SUBCLASS

COUNT 23

DISTRICT OF COLUMBIA CONSUMER SECURITY BREACH NOTIFICATION ACT, D.C. Code §§ 28-3851, *et seq.*

563. The District of Columbia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the District of Columbia Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

564. Equifax is a business that owns or licenses computerized data that includes Personal Information as defined by D.C. Code § 28-3852(a).

565. Plaintiff and District of Columbia Subclass members' Personal Information (*e.g.*, Social Security numbers) includes Personal Information as covered under D.C. Code § 28-3851(3).

566. Equifax is required to accurately notify Plaintiff and District of Columbia Subclass members if it becomes aware of a breach of its data security system in the most expedient time possible and without unreasonable delay under D.C. Code § 28-3852(a).

567. Because Equifax was aware of a breach of its security system, Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by D.C. Code § 28-3852(a).

568. By failing to disclose the Equifax data breach in a timely and accurate manner Equifax violated D.C. Code § 28-3852(a).

569. As a direct and proximate result of Equifax's violations of D.C. Code § 28-3852(a), Plaintiff and District of Columbia Subclass members suffered damages, as described above.

570. Plaintiff and District of Columbia Subclass members seek relief under D.C. Code § 28-3853(a), including actual damages.

COUNT 24

DISTRICT OF COLUMBIA CONSUMER PROTECTION PROCEDURES ACT, D.C. Code §§ 28-3904, *et seq.*

571. The District of Columbia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the District of Columbia Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

572. Equifax is a "person" as defined by D.C. Code § 28-3901(a)(1).

573. Equifax is a "merchant" as defined by D.C. Code § 28-3901(a)(3).

574. Plaintiff and District of Columbia Subclass members are "consumers" who purchased or received goods or services for personal, household, or family purposes, as defined by D.C. Code § 28-3901.

575. Equifax advertised, offered, or sold goods or services in District of Columbia and engaged in trade or commerce directly or indirectly affecting the people of District of Columbia.

576. Equifax engaged in unfair, unlawful, and deceptive trade practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of goods and services in violation of D.C. Code § 28-3904, 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, grade, style, or model, when they are of another;

c. Misrepresenting a material fact that has a tendency to mislead;

d. Failing to state a material fact where the failure is misleading;

e. Advertising or offering goods or services without the intent to sell them as advertised or offered; and

f. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

577. Equifax's unfair, unlawful, and deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and District of Columbia Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous

cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and District of Columbia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and District of Columbia Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and District of Columbia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and District of Columbia Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and District of Columbia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

578. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

579. Equifax intended to mislead Plaintiff and District of Columbia Subclass members and induce them to rely on its misrepresentations and omissions.

580. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and District of Columbia Subclass members that they could not

reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

581. Equifax acted intentionally, knowingly, and maliciously to violate the District of Columbia's Consumer Protection Procedures Act, and recklessly disregarded Plaintiff and District of Columbia Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

582. As a direct and proximate result of Equifax's unfair, unlawful, and deceptive trade practices, Plaintiff and District of Columbia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

583. Plaintiff and District of Columbia Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, restitution, injunctive relief, punitive damages, attorneys' fees and costs, the greater of treble damages or $1500 per violation, and any other relief that the Court deems proper.

CLAIMS ON BEHALF OF THE FLORIDA SUBCLASS

COUNT 25

FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT, Fla. Stat. §§ 501.201, *et seq.*

584. The Florida Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Florida Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

585. Plaintiff and Florida Subclass members are "consumers" as defined by Fla. Stat. § 501.203.

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

587. Equifax engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Florida Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately

improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Florida Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Florida's data security statute, F.S.A. § 501.171(2), which was a direct and proximate cause of the Equifax data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Florida Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Florida Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the

FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Florida's data security statute, F.S.A. § 501.171(2);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Florida Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Florida Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Florida's data security statute, F.S.A. § 501.171(2).

588. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

589. 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 serve as trusted linchpins of the financial system and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Florida Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the Florida Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

590. As a direct and proximate result of Equifax's unconscionable, unfair, and deceptive acts and practices, Plaintiff and Florida Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

591. Plaintiff and Florida Subclass members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages under Fla. Stat. § 501.21; declaratory and injunctive relief; reasonable attorneys' fees and costs, under Fla. Stat. § 501.2105(1); and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE GEORGIA SUBCLASS

COUNT 26

GEORGIA SECURITY BREACH NOTIFICATION ACT, O.C.G.A. §§ 10-1-912, *et seq.*

592. The Georgia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Georgia Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

593. Equifax is a business that owns or licenses computerized data that includes Personal Information as defined by O.C.G.A. § 10-1-912(a).

594. Plaintiff and Georgia Subclass members' Personal Information (*e.g.*, Social Security numbers) includes Personal Information as covered under O.C.G.A. § 10-1-912(a).

595. Equifax is required to accurately notify Plaintiff and Georgia Subclass members if it becomes aware of a breach of its data security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and

Georgia Subclass members' Personal Information, in the most expedient time possible and without unreasonable delay under O.C.G.A. § 10-1-912(a).

596. Because Equifax was aware of a breach of its security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Georgia Subclass members' Personal Information, Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by O.C.G.A. § 10-1-912(a).

597. By failing to disclose the Equifax data breach in a timely and accurate manner, Equifax violated O.C.G.A. § 10-1-912(a).

598. As a direct and proximate result of Equifax's violations of O.C.G.A. § 10-1-912(a), Plaintiff and Georgia Subclass members suffered damages, as described above.

599. Plaintiff and Georgia Subclass members seek relief under O.C.G.A. § 10-1-912 including actual damages and injunctive relief.

COUNT 27

GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT,

O.C.G.A. §§ 10-1-370, *et seq.*

600. The Georgia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Georgia Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

601. Equifax, Plaintiff, and Georgia Subclass members are "persons" within the meaning of § 10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA").

602. Equifax engaged in deceptive trade practices in the conduct of its business, in violation of O.C.G.A. § 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;

c. Advertising goods or services with intent not to sell them as advertised; and

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

603. Equifax's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Georgia Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and Georgia Subclass members'

Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Georgia Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

604. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data

security and ability to protect the confidentiality of consumers' Personal Information.

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

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

607. Equifax acted intentionally, knowingly, and maliciously to violate Georgia's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Georgia Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

608. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Georgia Subclass. Equifax accepted the responsibility of being a "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, 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.

609. 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, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

610. Plaintiff and Georgia Subclass members seek all relief allowed by law, including injunctive relief, and reasonable attorneys' fees and costs, under O.C.G.A. § 10-1-373.

CLAIMS ON BEHALF OF THE HAWAII SUBCLASS

COUNT 28

HAWAII SECURITY BREACH NOTIFICATION ACT, Haw. Rev. Stat. §§ 487N-1, *et seq.*

611. The Hawaii Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Hawaii Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

612. Equifax is a business that owns or licenses computerized data that includes Personal Information as defined by Haw. Rev. Stat. § 487N-2(a).

613. Plaintiff and Hawaii Subclass members' Personal Information (*e.g.*, Social Security numbers) includes Personal Information as covered under Haw. Rev. Stat. § 487N-2(a).

614. Equifax is a business that owns or licenses computerized data that includes Personal Information as defined by Haw. Rev. Stat. § 487N-2(a).

615. Plaintiff and Hawaii Subclass members' Personal Information (*e.g.*, Social Security numbers) includes Personal Information as covered under Haw. Rev. Stat. § 487N-2(a).

616. Equifax is required to accurately notify Plaintiff and Hawaii Subclass members if it becomes aware of a breach of its data security system without unreasonable delay under Haw. Rev. Stat. § 487N-2(a).

617. Because Equifax was aware of a breach of its security system, it had an obligation to disclose the Equifax data breach in a timely and accurate fashion as mandated by Haw. Rev. Stat. § 487N-2(a).

618. By failing to disclose the Equifax data breach in a timely and accurate manner, Equifax violated Haw. Rev. Stat. § 487N-2(a).

619. As a direct and proximate result of Equifax's violations of Haw. Rev. Stat. § 487N-2(a), Plaintiff and Hawaii Subclass members suffered damages, as described above.

620. Plaintiff and Hawaii Subclass members seek relief under Haw. Rev. Stat. § 487N-3(b), including actual damages.

COUNT 29

HAWAII UNFAIR PRACTICES AND UNFAIR COMPETITION ACT, Haw. Rev. Stat. §§ 480-1, *et seq.*

621. The Hawaii Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Hawaii Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

622. Plaintiff and Hawaii Subclass members are "consumers" as defined by Haw. Rev. Stat. § 480-1.

623. Plaintiffs, the Hawaii Subclass members, and Equifax are "persons" as defined by Haw. Rev. Stat. § 480-1.

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

625. Equifax engaged in unfair or deceptive acts or practices, misrepresentations, and the concealment, suppression, and omission of material facts with respect to the sale and advertisement of the goods and services purchased by Hawaii Subclass members in violation of Haw. Rev. Stat. § 480-2(a), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Hawaii Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties

imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Hawaii Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Hawaii Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties

imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

626. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

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

628. The foregoing unlawful and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous.

629. Equifax acted intentionally, knowingly, and maliciously to violate Hawaii's Unfair Practices and Unfair Competition Act, and recklessly disregarded Plaintiff and Hawaii Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

630. As a direct and proximate result of Equifax's deceptive acts and practices, Plaintiff and Hawaii Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased,

imminent risk of fraud and identity theft; and loss of value of their Personal Information.

631. Plaintiff and Hawaii Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, benefit of the bargain damages, treble damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT 30

HAWAII UNIFORM DECEPTIVE TRADE PRACTICE ACT, Haw. Rev. Stat. §§ 481A-3, *et seq.*

632. The Hawaii Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Hawaii Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

633. Plaintiff and Hawaii Subclass members are "persons" as defined by Haw. Rev. Stat. § 481A-2.

634. Equifax engaged in unfair and deceptive trade practices in the conduct of its business, violating Haw. Rev. Stat. § 481A-3, 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;

c. Advertising goods or services with intent not to sell them as advertised; and

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

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

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Hawaii Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Hawaii Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Hawaii Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Hawaii Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

636. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

637. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Hawaii Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

638. As a direct and proximate result of Equifax's unfair, unlawful, and deceptive trade practices, Plaintiff and Hawaii Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

639. Plaintiff and Hawaii Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, attorneys' fees and costs, and any other relief that the Court deems proper.

CLAIMS ON BEHALF OF THE IDAHO SUBCLASS

COUNT 31

IDAHO CONSUMER PROTECTION ACT, Idaho Code §§ 48-601, *et seq.*

640. The Idaho Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Idaho Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

641. Equifax is a "person" as defined by Idaho Code § 48-602(1).

642. Equifax's conduct as alleged herein pertained to "goods" and "services" as defined by Idaho Code § 48-602(6) and (7).

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

644. Equifax engaged in unfair and deceptive acts or practices, and unconscionable acts and practices, in the conduct of trade and commerce with respect to the sale and advertisement of goods and services, in violation of Idaho Code §§ 48-603 and 48-603(C), including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have;

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

c. Advertising goods or services with intent not to sell them as advertised;

d. Engaging in other acts and practices that are otherwise misleading, false, or deceptive to consumers; and

e. Engaging in unconscionable methods, acts or practices in the conduct of trade or commerce.

645. Equifax's unfair, deceptive, and unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Idaho Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Idaho Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Idaho Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Idaho Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Idaho Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Idaho Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

646. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

647. Equifax intended to mislead Plaintiff and Idaho Subclass members and induce them to rely on its misrepresentations and omissions. Equifax knew its representations and omissions were false.

648. Equifax acted intentionally, knowingly, and maliciously to violate Idaho's Consumer Protection Act, and recklessly disregarded Plaintiff and Idaho Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

649. As a direct and proximate result of Equifax's unfair, deceptive, and unconscionable conduct, Plaintiff and Idaho Subclass members have suffered and

will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

650. Plaintiff and Idaho Subclass members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, injunctive relief, costs, and attorneys' fees.

CLAIMS ON BEHALF OF THE ILLINOIS SUBCLASS

COUNT 32

ILLINOIS PERSONAL INFORMATION PROTECTION ACT, 815 Ill. Comp. Stat. §§ 530/10(a), *et seq.*

651. The Illinois Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

652. As a publicly held corporation which handles, collects, disseminates, and otherwise deals with nonpublic personal information, Equifax is a Data Collector as defined in 815 Ill. Comp. Stat. § 530/5.

653. Plaintiff and Illinois Subclass members' Personal Information (*e.g.*, Social Security numbers) includes Personal Information as covered under 815 Ill. Comp. Stat. § 530/5.

654. As a Data Collector, Equifax is required to notify Plaintiff and Illinois Subclass members of a breach of its data security system in the most expedient time possible and without unreasonable delay pursuant to 815 Ill. Comp. Stat. § 530/10(a).

655. By failing to disclose the Equifax data breach in the most expedient time possible and without unreasonable delay, Equifax violated 815 Ill. Comp. Stat. § 530/10(a).

656. Pursuant to 815 Ill. Comp. Stat. § 530/20, a violation of 815 Ill. Comp. Stat. § 530/10(a) constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

657. As a direct and proximate result of Equifax's violations of 815 Ill. Comp. Stat. § 530/10(a), Plaintiff and Illinois Subclass members suffered damages, as described above.

658. Plaintiff and Connecticut Subclass members seek relief under 815 Ill. Comp. Stat. § 510/3 for the harm they suffered because of Equifax's willful

violations of 815 Ill. Comp. Stat. § 530/10(a), including actual damages, equitable relief, costs, and attorneys' fees.

COUNT 33

ILLINOIS CONSUMER FRAUD ACT, 815 Ill. Comp. Stat. §§ 505, *et seq.*

659. The Illinois Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

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

661. Plaintiff and Illinois Subclass members are "consumers" as defined by 815 Ill. Comp. Stat. §§ 505/1(e).

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

663. Equifax's deceptive, unfair, and unlawful trade acts or practices, in violation of 815 Ill. Comp. Stat. § 505/2, include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Illinois Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Equifax data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Illinois Subclass members'

Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Illinois Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Personal Information, including duties

imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

664. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

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

666. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that these consumers could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

667. Equifax acted intentionally, knowingly, and maliciously to violate Illinois's Consumer Fraud Act, and recklessly disregarded Plaintiff and Illinois

Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

668. As a direct and proximate result of Equifax's unfair, unlawful, and deceptive acts and practices, Plaintiff and Illinois Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

669. Plaintiff and Illinois Subclass members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, injunctive relief, and reasonable attorneys' fees and costs.

COUNT 34

ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT, 815 Ill. Comp. Stat. §§ 510/2, *et seq.*

670. The Illinois Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Illinois Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

671. Equifax is a "person" as defined by 815 Ill. Comp. Stat. §§ 510/1(5).

672. 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;

c. Advertising goods or services with intent not to sell them as advertised; and

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

673. Equifax's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Illinois Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous

cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a), which was a direct and proximate cause of the Equifax data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Illinois Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of

Plaintiff and Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Illinois Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Illinois Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, the Illinois Insurance Information and Privacy Protection Act, 215 Ill. Comp. Stat. § 5/1014, Illinois laws regulating the use and

disclosure of Social Security Numbers, 815 Ill. Comp. Stat § 505/2RR, and the Illinois Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 510/2(a).

674. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

675. The above unfair and deceptive practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Illinois Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

676. 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, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

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

CLAIMS ON BEHALF OF THE INDIANA SUBCLASS

COUNT 35

INDIANA DECEPTIVE CONSUMER SALES ACT, Ind. Code §§ 24-5-0.5-1, *et seq.*

678. The Indiana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Indiana Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

679. Equifax is a "person" as defined by Ind. Code § 24-5-0.5-2(a)(2).

680. Equifax is a "supplier" as defined by § 24-5-0.5-2(a)(1), because it regularly engages in or solicits "consumer transactions," within the meaning of § 24-5-0.5-2(a)(3)(A).

681. Equifax engaged in unfair, abusive, and deceptive acts, omissions, and practices in connection with consumer transactions, in violation of Ind. Code § 24-5-0.5-3(a).

682. Equifax's representations and omissions include both implicit and explicit representations.

683. Equifax's unfair, abusive, and deceptive acts, omissions, and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Indiana Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Indiana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Indiana security breach law, Ind. Code § 24-4.9-3-3.5(c), which was a direct and proximate cause of the Equifax data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Indiana Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Indiana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Indiana security breach law, Ind. Code § 24-4.9-3-3.5(c);

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Indiana Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Indiana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C.

§ 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Indiana security breach law, Ind. Code § 24-4.9-3-3.5(c).

684. Equifax's acts and practices were "unfair" because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

685. The injury to consumers from Equifax's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and an unwarranted risk to the safety of their Personal Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

686. Consumers could not have reasonably avoided injury because Equifax's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Equifax created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury. Equifax's

business acts and practices also took advantage of its special status as one the nation's three major credit bureaus, making it functionally impossible for consumers to obtain credit without their Personal Information being in Equifax's systems.

687. Equifax's inadequate data security had no countervailing benefit to consumers or to competition.

688. Equifax's acts and practices were "abusive" for numerous reasons, including:

a. Because they materially interfered with consumers' ability to understand a term or condition in a consumer transaction. Equifax's failure to disclose the inadequacies in its data security interfered with consumers' decision-making in a variety of their transactions.

b. Because they took unreasonable advantage of consumers' lack of understanding about the material risks, costs, or conditions of a consumer transaction. Without knowing about the inadequacies in Equifax's data security, consumers lacked an understanding of the material risks and costs of a variety of their transactions.

c. Because they took unreasonable advantage of consumers' inability to protect their own interests. Consumers could not protect their interests due to the asymmetry in information between them and Equifax concerning the state of Equifax's security, and because it is functionally impossible for consumers to obtain credit without their Personal Information being in Equifax's systems.

d. Because Equifax took unreasonable advantage of consumers' reasonable reliance that it was acting in their interests to secure their data. Consumers' reliance was reasonable for the reasons discussed four paragraphs below.

689. Equifax also engaged in "deceptive" acts and practices in violation of Indiana Code § 24-5-0.5-3(a) and § 24-5-0.5-3(b), including:

a. Misrepresenting that the subject of a consumer transaction has sponsorship, approval, performance, characteristics, accessories, uses, or benefits it does not have which the supplier knows or should reasonably know it does not have;

b. Misrepresenting that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not

and if the supplier knows or should reasonably know that it is not; and

c. Misrepresenting that the subject of a consumer transaction will be supplied to the public in greater quantity (i.e., more data security) than the supplier intends or reasonably expects.

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

691. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

692. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Indiana Subclass. Equifax accepted the responsibility of

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

693. Equifax had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the Personal Information in its possession, and the generally accepted professional standards in the credit reporting industry. This duty arose because members of the public, including Plaintiff and the Indiana Subclass, repose a trust and confidence in Equifax as one of the nation's entrusted "stewards of data" and Equifax's position as one of three nationwide credit-reporting companies that serve as linchpins of the financial system. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Indiana Subclass—and Equifax, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Equifax. Equifax's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Indiana Subclass that contradicted these representations.

694. Equifax acted intentionally, knowingly, and maliciously to violate Indiana's Deceptive Consumer Sales Act, and recklessly disregarded Plaintiff and Indiana Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate. Equifax's actions were not the result of a mistake of fact or law, honest error or judgment, overzealousness, mere negligence, or other human failing.

695. Plaintiff sent a demand for relief on behalf of the Indiana Subclass pursuant to Ind. Code § 24-5-0.5-5 on October 10, 2017. Equifax has not cured its unfair, abusive, and deceptive acts and practices, or its violations of Indiana Deceptive Consumer Sales Act were incurable.

696. Since Plaintiff provided the requisite notice, Equifax has failed to cure its violations of the Indiana Deceptive Consumer Sales Act.

697. Equifax's conduct includes incurable deceptive acts that Equifax engaged in as part of a scheme, artifice, or device with intent to defraud or mislead, under Ind. Code § 24-5-0.5-2(a)(8).

698. As a direct and proximate result of Equifax's uncured or incurable unfair, abusive, and deceptive acts or practices, Plaintiff and Indiana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

699. Equifax's violations present a continuing risk to Plaintiff and Indiana Subclass members as well as to the general public.

700. Plaintiff and Indiana Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $500 for each non-willful violation; the greater of treble damages or $1,000 for each willful violation; restitution; reasonable attorneys' fees and costs; injunctive relief; and punitive damages.

CLAIMS ON BEHALF OF THE IOWA SUBCLASS

COUNT 36

PERSONAL INFORMATION SECURITY BREACH PROTECTION LAW, Iowa Code § 715C.2

701. The Iowa Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Iowa Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

702. Equifax is a business that owns or licenses computerized data that includes Personal Information as defined by Iowa Code § 715C.2(1).

703. Plaintiff's and Iowa Subclass members' Personal Information (*e.g.*, Social Security numbers) includes Personal Information as covered under Iowa Code § 715C.2(1).

704. Equifax is required to accurately notify Plaintiff and Iowa Subclass members if it becomes aware of a breach of its data security system in the most expeditious time possible and without unreasonable delay under Iowa Code § 715C.2(1).

705. Because Equifax was aware of a breach of its security system, Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Iowa Code § 715C.2(1).

706. By failing to disclose the Equifax data breach in a timely and accurate manner, Equifax violated Iowa Code § 715C.2(1).

707. Pursuant to Iowa Code § 715C.2(9), a violation of Iowa Code § 715C.2(1) is an unlawful practice pursuant to Iowa Code Ann. § 714.16(7).

708. As a direct and proximate result of Equifax's violations of Iowa Code § 715C.2(1), Plaintiff and Iowa Subclass members suffered damages, as described above.

709. Plaintiff and Iowa Subclass members seek relief under Iowa Code § 714.16(7), including actual damages and injunctive relief.

COUNT 37

IOWA PRIVATE RIGHT OF ACTION FOR CONSUMER FRAUDS ACT, Iowa Code § 714H

710. The Iowa Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Iowa Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

711. Equifax is a "person" as defined by Iowa Code § 714H.2(7).

712. Plaintiff and Iowa Subclass members are "consumers" as defined by Iowa Code § 714H.2(3).

713. Equifax's conduct described herein related to the "sale" or "advertisement" of "merchandise" as defined by Iowa Code §§ 714H.2(2), (6), & (8).

714. Equifax engaged in unfair, deceptive, and unconscionable trade practices, in violation of the Iowa Private Right of Action for Consumer Frauds Act, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Iowa Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Iowa Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C.

§ 1681e, 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 the privacy and confidentiality of Plaintiff and Iowa Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Iowa Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Iowa Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Iowa Subclass members' Personal Information, including duties

imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

715. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

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

717. Equifax acted intentionally, knowingly, and maliciously to violate Iowa's Private Right of Action for Consumer Frauds Act, and recklessly disregarded Plaintiff and Iowa Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

718. As a direct and proximate result of Equifax's unfair, deceptive, and unconscionable conduct, Plaintiff and Iowa Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity;

an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

719. Plaintiff has provided the requisite notice to the Iowa Attorney General, the office of which approved the filing of this class action lawsuit pursuant to Iowa Code § 714H.7.

720. Plaintiff and Iowa Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, punitive damages, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE KANSAS SUBCLASS

COUNT 38

PROTECTION OF CONSUMER INFORMATION, Kan. Stat. Ann. §§ 50-7a02(a), *et seq.*

721. The Kansas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kansas Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

722. Equifax is a business that owns or licenses computerized data that includes Personal Information as defined by Kan. Stat. Ann. § 50-7a02(a).

723. Plaintiff's and Kansas Subclass members' Personal Information (*e.g.*, Social Security numbers) includes Personal Information as covered under Kan. Stat. Ann. § 50-7a02(a).

724. Equifax is required to accurately notify Plaintiffs and Kansas Subclass members if it becomes aware of a breach of its data security system that was reasonably likely to have caused misuse of Plaintiff's and Kansas Subclass members' Personal Information, in the most expedient time possible and without unreasonable delay under Kan. Stat. Ann. § 50-7a02(a).

725. Because Equifax was aware of a breach of its security system that was reasonably likely to have caused misuse of Plaintiffs' and Kansas Subclass members' Personal Information, Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Kan. Stat. Ann. § 50-7a02(a).

726. By failing to disclose the Equifax data breach in a timely and accurate manner, Equifax violated Kan. Stat. Ann. § 50-7a02(a).

727. As a direct and proximate result of Equifax's violations of Kan. Stat. Ann. § 50-7a02(a), Plaintiff and Kansas Subclass members suffered damages, as described above.

728. Plaintiff and Kansas Subclass members seek relief under Kan. Stat. Ann. § 50-7a02(g), including equitable relief.

COUNT 39

KANSAS CONSUMER PROTECTION ACT, K.S.A. §§ 50-623, *et seq.*

729. The Kansas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kansas Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

730. K.S.A. §§ 50-623, *et seq.* is to be liberally construed to protect consumers from suppliers who commit deceptive and unconscionable practices.

731. Plaintiff and Kansas Subclass members are "consumers" as defined by K.S.A. § 50-624(b).

732. The acts and practices described herein are "consumer transactions," as defined by K.S.A. § 50-624(c).

733. Equifax is a "supplier" as defined by K.S.A. § 50-624(l).

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

735. Equifax engaged in deceptive and unfair acts or practices, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Kansas Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b, which was a direct and proximate cause of the Equifax data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Kansas Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of

Plaintiff and Kansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Kansas Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kansas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Kansas's identity fraud statute, the Wayne Owen Act, K.S.A. § 50-6,139b.

736. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data

security and ability to protect the confidentiality of consumers' Personal Information.

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

738. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Kansas Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the Kansas Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

739. Equifax also engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of K.S.A. § 50-627, including:

a. Knowingly taking advantage of the inability of Plaintiff and the Kansas Subclass to reasonably protect their interests, due to their lack of knowledge (see K.S.A. § 50-627(b)(1)); and

b. Requiring Plaintiff and the Kansas Subclass to enter into a consumer transaction on terms that Equifax knew were substantially one-sided in favor of Equifax (see K.S.A. § 50-627(b)(5)).

740. Plaintiff and the Kansas Subclass had unequal bargaining power with respect to their ability to control the security and confidentiality of their Personal Information in Equifax's possession.

741. The above unfair, deceptive, and unconscionable practices and acts by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kansas Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

742. Equifax acted intentionally, knowingly, and maliciously to violate Kansas's Consumer Protection Act, and recklessly disregarded Plaintiff and Kansas Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

743. As a direct and proximate result of Equifax's unfair, deceptive, and unconscionable trade practices, Plaintiff and Kansas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

744. Plaintiff and Kansas Subclass members seek all monetary and non-monetary relief allowed by law, including civil penalties or actual damages (whichever is greater), under K.S.A. §§ 50-634 and 50-636; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE KENTUCKY SUBCLASS

COUNT 40

KENTUCKY COMPUTER SECURITY BREACH NOTIFICATION ACT, Ky. Rev. Stat. Ann. §§ 365.732, *et seq.*

745. The Kentucky Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kentucky Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

746. Equifax is required to accurately notify Plaintiff and Kentucky Subclass members if it becomes aware of a breach of its data security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Kentucky Subclass members' Personal Information, in the most expedient time possible and without unreasonable delay under Ky. Rev. Stat. Ann. § 365.732(2).

747. Equifax is a business that holds computerized data that includes Personal Information as defined by Ky. Rev. Stat. Ann. § 365.732(2).

748. Plaintiff's and Kentucky Subclass members' Personal Information includes Personal Information as covered under Ky. Rev. Stat. Ann. § 365.732(2).

749. Because Equifax was aware of a breach of its security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Kentucky Subclass members' Personal Information, Equifax had an obligation to

disclose the data breach in a timely and accurate fashion as mandated by Ky. Rev. Stat. Ann. § 365.732(2).

750. By failing to disclose the Equifax data breach in a timely and accurate manner, Equifax violated Ky. Rev. Stat. Ann. § 365.732(2).

751. As a direct and proximate result of Equifax's violations of Ky. Rev. Stat. Ann. § 365.732(2), Plaintiff and Kentucky Subclass members suffered damages, as described above.

752. Plaintiff and Kentucky Subclass members seek relief under Ky. Rev. Stat. Ann. § 446.070, including actual damages.

COUNT 41

KENTUCKY CONSUMER PROTECTION ACT, Ky. Rev. Stat. §§ 367.110, *et seq.*

753. The Kentucky Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Kentucky Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

754. Equifax is a "person" as defined by Ky. Rev. Stat. § 367.110(1).

755. Equifax advertised, offered, or sold goods or services in Kentucky and engaged in trade or commerce directly or indirectly affecting the people of Kentucky, as defined by Ky. Rev. Stat. 367.110(2).

756. Equifax engaged in unfair, false, misleading, deceptive, and unconscionable acts or practices, in violation of Ky. Rev. Stat. § 367.170, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Kentucky Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kentucky Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and Kentucky Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kentucky Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Kentucky Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Kentucky Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

757. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

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

759. Plaintiff and Kentucky Subclass members' purchased goods or services for personal, family, or household purposes and suffered ascertainable losses of money or property as a result of Equifax's unlawful acts and practices.

760. The above unlawful acts and practices by Equifax were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kentucky Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

761. Equifax acted intentionally, knowingly, and maliciously to violate Kentucky's Consumer Protection Act, and recklessly disregarded Plaintiff and Kentucky Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

762. As a direct and proximate result of Equifax's unlawful acts and practices, Plaintiff and Kentucky Subclass members have suffered and will

continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

763. Plaintiff and Kentucky Subclass members seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, restitution or other equitable relief, injunctive relief, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE LOUISIANA SUBCLASS

COUNT 42

DATABASE SECURITY BREACH NOTIFICATION LAW, La. Rev. Stat. Ann. §§ 51:3074(A), *et seq.*

764. The Louisiana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Louisiana Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

765. Equifax is a business that owns or licenses computerized data that includes Personal Information as defined by La. Rev. Stat. Ann. § 51:3074(C).

766. Plaintiff's and Louisiana Subclass members' Personal Information (*e.g.*, Social Security numbers) includes Personal Information as covered under La. Rev. Stat. Ann. § 51:3074(C).

767. Equifax is required to accurately notify Plaintiff and Louisiana Subclass members if it becomes aware of a breach of its data security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Louisiana Subclass members' Personal Information, in the most expedient time possible and without unreasonable delay under La. Rev. Stat. Ann. § 51:3074(C).

768. Because Equifax was aware of a breach of its security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff's and Louisiana Subclass members' Personal Information, Equifax had an obligation to disclose the Equifax data breach in a timely and accurate fashion as mandated by La. Rev. Stat. Ann. § 51:3074(C).

769. By failing to disclose the Equifax data breach in a timely and accurate manner, Equifax violated La. Rev. Stat. Ann. § 51:3074(C).

770. As a direct and proximate result of Equifax's violations of La. Rev. Stat. Ann. § 51:3074(C), Plaintiff and Louisiana Subclass members suffered damages, as described above.

771. Plaintiff and Louisiana Subclass members seek relief under La. Rev. Stat. Ann. § 51:3075, including actual damages.

COUNT 43

LOUISIANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, La. Rev. Stat. Ann. §§ 51:1401, *et seq.*

772. The Louisiana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Louisiana Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

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

774. Plaintiff and Louisiana Subclass members are "consumers" within the meaning of La. Rev. Stat. Ann. § 51:1402(1).

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

776. The Louisiana Unfair Trade Practices and Consumer Protection Law ("Louisiana CPL") makes unlawful "unfair or deceptive acts or practices in the conduct of any trade or commerce." La. Rev. 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.

777. Equifax participated in unfair and deceptive acts and practices that violated the Louisiana CPL, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Louisiana Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and Louisiana Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Louisiana Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Louisiana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

778. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

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

780. Equifax's unfair and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Kentucky Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

781. Equifax acted intentionally, knowingly, and maliciously to violate Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Louisiana Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

782. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Louisiana Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the Louisiana Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

783. 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, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

784. 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 Louisiana CPL; declaratory relief; attorneys' fees; and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE MAINE SUBCLASS

COUNT 44

MAINE UNFAIR TRADE PRACTICES ACT, 5 Me. Rev. Stat. §§ 205, 213, *et seq.*

785. The Maine Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Maine Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

786. Equifax is a "person" as defined by 5 Me. Stat. § 206(2).

787. Equifax's conduct as alleged herein related was in the course of "trade and commerce" as defined by 5 Me. Stat. § 206(3).

788. Plaintiff and Maine Subclass members purchased goods and/or services for personal, family, and/or household purposes.

789. Plaintiff sent a demand for relief on behalf of the Maine Subclass pursuant to 5 Me. Rev. Stat. § 213(1-A) on October 10, 2017.

790. Equifax engaged in unfair and deceptive trade acts and practices in the conduct of trade or commerce, in violation of 5 Me. Rev. Stat. §207, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Maine Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and Maine Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the

FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Maine Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

791. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

792. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Maine Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the Maine Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

793. As a direct and proximate result of Equifax's unfair and deceptive acts and conduct, Plaintiff and Maine Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

794. Plaintiff and the Maine Subclass members seek all monetary and non-monetary relief allowed by law, including damages or restitution, injunctive and other equitable relief, and attorneys' fees and costs.

COUNT 45

MAINE UNIFORM DECEPTIVE TRADE PRACTICES ACT, 10 Me. Rev. Stat. §§ 1212, *et seq.*

795. The Maine Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Maine Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

796. Equifax is a "person" as defined by 10 Me. Rev. Stat. § 1211(5).

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

798. Equifax engaged in deceptive trade practices in the conduct of its business, in violation of 10 Me. Rev. Stat. §1212, 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;

c. Advertising goods or services with intent not to sell them as advertised; and

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

799. Equifax's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Maine Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and Maine Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Maine Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maine Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

800. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

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

802. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Maine Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the Maine Subclass members acted reasonably in relying on

Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

803. As a direct and proximate result of Equifax's deceptive trade practices, Plaintiff and Maine Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

804. Maine Subclass members are likely to be damaged by Equifax's ongoing deceptive trade practices.

805. Plaintiff and the Maine Subclass members seek all monetary and non-monetary relief allowed by law, including damages or restitution, injunctive or other equitable relief, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE MARYLAND SUBCLASS

COUNT 46

MARYLAND PERSONAL INFORMATION PROTECTION ACT, Md. Comm. Code §§ 14-3501, *et seq.*

806. The Maryland Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Maryland Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

807. Under Md. Comm. Code § 14-3503(a), "[t]o protect Personal Information from unauthorized access, use, modification, or disclosure, a business that owns or licenses Personal Information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of Personal Information owned or licensed and the nature and size of the business and its operations."

808. Equifax is a business that owns or licenses computerized data that includes Personal Information as defined by Md. Comm. Code §§ 14-3501(b)(1) and (2).

809. Plaintiff and Maryland Subclass members are "individuals" and "customers" as defined and covered by Md. Comm. Code §§ 14-3502(a) and 14-3503.

810. Plaintiff's and Maryland Subclass members' Personal Information includes Personal Information as covered under Md. Comm. Code § 14-3501(d).

811. Equifax did not maintain reasonable security procedures and practices appropriate to the nature of the Personal Information owned or licensed and the nature and size of its business and operations in violation of Md. Comm. Code § 14-3503.

812. The Equifax data breach was a "breach of the security of a system" as defined by Md. Comm. Code § 14-3504(1).

813. Under Md. Comm. Code § 14-3504(b)(1), "[a] business that owns or licenses computerized data that includes Personal Information of an individual residing in the State, when it discovers or is notified of a breach of the security system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that Personal Information of the individual has been or will be misused as a result of the breach."

814. Under Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), "[i]f, after the investigation is concluded, the business determines that misuse of the individual's Personal Information has occurred or is reasonably likely to occur as a result of a breach of the security system, the business shall notify the individual of

the breach" and that notification "shall be given as soon as reasonably practical after the business discovers or is notified of the breach of a security system."

815. Because Equifax discovered a security breach and had notice of a security breach, Equifax had an obligation to disclose the Equifax data breach in a timely and accurate fashion as mandated by Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

816. By failing to disclose the Equifax data breach in a timely and accurate manner, Equifax violated Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2).

817. As a direct and proximate result of Equifax's violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2), Plaintiff and Maryland Subclass members suffered damages, as described above.

818. Pursuant to Md. Comm. Code § 14-3508, Equifax's violations of Md. Comm. Code §§ 14-3504(b)(2) and 14-3504(c)(2) are unfair or deceptive trade practices within the meaning of the Maryland Consumer Protection Act, 13 Md. Comm. Code §§ 13-101, *et seq.* and subject to the enforcement and penalty provisions contained within the Maryland Consumer Protection Act.

819. Plaintiff and Maryland Subclass members seek relief under Md. Comm. Code §13-408, including actual damages and attorney's fees.

COUNT 47

MARYLAND SOCIAL SECURITY NUMBER PRIVACY ACT, Md. Comm. Code §§ 14-3401, *et seq.*

820. The Maryland Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Maryland Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

821. Equifax is a "person" as covered by Md. Comm. Code § 14-3402.

822. Plaintiff and Maryland Subclass members are "individual[s]" covered by Md. Comm. Code § 14-3402.

823. Md. Comm. Code § 14-3402 prohibits a person from requiring an individual to transmit his/her Social Security number over the Internet unless the connection is secure or the individual's Social Security number is encrypted, and from initiating the transmission of an individual's Social Security number over the Internet unless the connection is secure or the Social Security number is encrypted.

824. As described above, Equifax transmitted Plaintiff's and Maryland Subclass members' Social Security numbers over the Internet on unsecure connections and/or without encrypting the Social Security Numbers in violation of Md. Comm. Code § 14-3402.

825. As a direct and proximate result of Equifax's violations of Md. Comm. Code § 14-3402, Plaintiff and Maryland Subclass members suffered damages, as described above.

826. Plaintiff and Maryland Subclass members seek relief under Md. Comm. Code § 14-3402, including actual damages and attorneys' fees.

COUNT 48

MARYLAND CONSUMER PROTECTION ACT, Md. Comm. Code §§ 13-301, *et seq.*

827. The Maryland Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Maryland Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

828. Equifax is a person as defined by Md. Comm. Code § 13-101(h).

829. Equifax's conduct as alleged herein related to "sales," "offers for sale," or "bailment" as defined by Md. Comm. Code § 13-101(i) and § 13-303.

830. Maryland Subclass members are "consumers" as defined by Md. Comm. Code § 13-101(c).

831. Equifax' advertises, offers, or sell "consumer goods" or "consumer services" as defined by Md. Comm. Code § 13-101(d).

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

833. Equifax engaged in unfair and deceptive trade practices, in violation of Md. Comm. Code § 13-301, including:

a. False or misleading oral or written representations that have the capacity, tendency, or effect of deceiving or misleading consumers;

b. Representing that consumer goods or services have a characteristic that they do not have;

c. Representing that consumer goods or services are of a particular standard, quality, or grade that they are not;

d. Failing to state a material fact where the failure deceives or tends to deceive;

e. Advertising or offering consumer goods or services without intent to sell, lease, or rent them as advertised or offered;

f. Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer

rely on the same in connection with the promotion or sale of consumer goods or services or the subsequent performance with respect to an agreement, sale lease or rental.

834. Equifax engaged in these unfair and deceptive trade practices in connection with offering for sale or selling consumer goods or services or with respect to the extension of consumer credit, in violation of Md. Comm. Code § 13-303, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Maryland Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maryland Subclass members' Personal Information, including duties

imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503, which was a direct and proximate cause of the Equifax data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Maryland Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maryland Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Maryland Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Maryland Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and the Maryland Personal Information Protection Act, Md. Comm. Code § 14-3503.

835. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information. Equifax's misrepresentations and omissions would have been important to a significant number of consumers in making financial decisions.

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

837. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Maryland Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the Maryland Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

838. Equifax acted intentionally, knowingly, and maliciously to violate Maryland's Consumer Protection Act, and recklessly disregarded Plaintiff and Maryland Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

839. As a direct and proximate result of Equifax's unfair and deceptive acts and practices, Plaintiff and Maryland Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an

increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

840. Plaintiff and Maryland Subclass members seek all monetary and non-monetary relief allowed by law, including damages, disgorgement, injunctive relief, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE MASSACHUSETTS SUBCLASS

COUNT 49

MASSACHUSETTS CONSUMER PROTECTION ACT, Mass. Gen. Laws Ann. Ch. 93A, §§ 1, *et seq.*

841. The Massachusetts Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Massachusetts Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

842. Equifax and Massachusetts Subclass members are "persons" as meant by Mass. Gen. Laws. Ann. Ch. 93A, § 1(a).

843. Equifax operates in "trade or commerce" as meant by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

844. Equifax advertised, offered, or sold goods or services in Massachusetts and engaged in trade or commerce directly or indirectly affecting the people of Massachusetts, as defined by Mass. Gen. Laws Ann. Ch. 93A, § 1(b).

845. Plaintiff sent a demand for relief on behalf of the Massachusetts Subclass pursuant to Mass. Gen. Laws Ann. Ch. 93A § 9(3) on October 10, 2017.

846. Equifax engaged in unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, in violation of Mass. Gen. Laws Ann. Ch. 93A, § 2(a), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Massachusetts Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Massachusetts Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et*

seq., and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05, which was a direct and proximate cause of the Equifax data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Massachusetts Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Massachusetts Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Massachusetts Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Massachusetts Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and the Massachusetts Data Security statute and its implementing regulations, Mass. Gen. Laws Ann. Ch. 93H, § 2; 201 Mass. Code Regs. 17.01-05.

847. Equifax's acts and practices were "unfair" because they fall within the penumbra of common law, statutory, and established concepts of unfairness, given that Equifax solely held the true facts about its inadequate security for Personal Information, which Plaintiff and the Massachusetts Subclass members could not independently discover.

848. Consumers could not have reasonably avoided injury because Equifax's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Equifax created an asymmetry of information between it and consumers that

precluded consumers from taking action to avoid or mitigate injury. Equifax's business acts and practices also took advantage of its special status as one the nation's three major credit bureaus, making it functionally impossible for consumers to obtain credit without their Personal Information being in Equifax's systems.

849. Equifax's inadequate data security had no countervailing benefit to consumers or to competition.

850. Equifax intended to mislead Plaintiff and Massachusetts Subclass members and induce them to rely on its misrepresentations and omissions. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

851. Equifax acted intentionally, knowingly, and maliciously to violate Massachusetts's Consumer Protection Act, and recklessly disregarded Plaintiff and Massachusetts Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

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

monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

853. Plaintiff and Massachusetts Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, double or treble damages, injunctive or other equitable relief, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE MICHIGAN SUBCLASS

COUNT 50

MICHIGAN IDENTITY THEFT PROTECTION ACT, Mich. Comp. Laws Ann. §§ 445.72, *et seq.*

854. The Michigan Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Michigan Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

855. Equifax is a business that owns or licenses computerized data that includes Personal Information as defined by Mich. Comp. Laws Ann. § 445.72(1).

856. Plaintiff's and Michigan Subclass members' Personal Information (*e.g.*, Social Security numbers) includes Personal Information as covered under Mich. Comp. Laws Ann. § 445.72(1).

857. Equifax is required to accurately notify Plaintiff and Michigan Subclass members if it discovers a security breach, or receives notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), without unreasonable delay under Mich. Comp. Laws Ann. § 445.72(1).

858. Because Equifax discovered a security breach and had notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), Equifax had an obligation to disclose the Equifax data breach in a timely and accurate fashion as mandated by Mich. Comp. Laws Ann. § 445.72(4).

859. By failing to disclose the Equifax data breach in a timely and accurate manner, Equifax violated Mich. Comp. Laws Ann. § 445.72(4).

860. As a direct and proximate result of Equifax's violations of Mich. Comp. Laws Ann. § 445.72(4), Plaintiff and Michigan Subclass members suffered damages, as described above.

861. Plaintiff and Michigan Subclass members seek relief under Mich. Comp. Laws Ann. § 445.72(13), including a civil fine.

COUNT 51

MICHIGAN CONSUMER PROTECTION ACT, Mich. Comp. Laws Ann. §§ 445.903, *et seq.*

862. The Michigan Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Michigan Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

863. Equifax and Michigan Subclass members are "persons" as defined by Mich. Comp. Laws Ann. § 445.903(d).

864. Equifax advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp. Laws Ann. § 445.903(g).

865. Equifax engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp. Laws Ann. § 445.903(1), including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have, in violation of Mich. Comp. Laws Ann. § 445.903(1)(c);

b. Representing that its goods and services are of a particular standard or quality if they are of another in violation of Mich. Comp. Laws Ann. § 445.903(1)(e);

c. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is, in violation of Mich. Comp. Laws Ann. § 445.903(1)(bb); and

d. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive matter, in violation of Mich. Comp. Laws Ann. § 445.903(1)(cc).

866. Equifax's unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Michigan Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Michigan Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and Michigan Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Michigan Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Michigan Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Michigan Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

867. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

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

869. Equifax acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Plaintiff and Michigan Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

870. As a direct and proximate result of Equifax's unfair, unconscionable, and deceptive practices, Plaintiff and Michigan Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and

monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

871. Plaintiff and Michigan Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $250, injunctive relief, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE MINNESOTA SUBCLASS

COUNT 52

MINNESOTA CONSUMER FRAUD ACT, Minn. Stat. §§ 325F.68, *et seq.* and Minn. Stat. §§ 8.31, *et seq.*

872. The Minnesota Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Minnesota Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

873. Equifax, Plaintiff, and members of the Minnesota Subclass are each a "person" as defined by Minn. Stat. § 325F.68(3).

874. Equifax's goods, services, commodities, and intangibles are "merchandise" as defined by Minn. Stat. § 325F.68(2).

875. Equifax engaged in "sales" as defined by Minn. Stat. § 325F.68(4).

876. Equifax engaged in fraud, false pretense, false promise, misrepresentation, misleading statements, and deceptive practices in connection with the sale of merchandise, in violation of Minn. Stat. § 325F.69(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Minnesota Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and Minnesota Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Minnesota Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

877. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

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

879. Equifax's fraudulent, misleading, and deceptive practices affected the public interest, including millions of Minnesotans affected by the Equifax Data Breach.

880. As a direct and proximate result of Equifax's fraudulent, misleading, and deceptive practices, Plaintiff and Minnesota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

881. Plaintiff and Minnesota Subclass members seek all monetary and non-monetary relief allowed by law, including damages; injunctive or other equitable relief; and attorneys' fees, disbursements, and costs.

COUNT 53

MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT, Minn. Stat. §§ 325D.43, *et seq.*

882. The Minnesota Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Minnesota Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

883. By engaging in deceptive trade practices in the course of its business and vocation, directly or indirectly affecting the people of Minnesota, Equifax violated Minn. Stat. § 325D.44, including the following provisions:

a. Representing that its goods and services had characteristics, uses, and benefits that they did not have, in violation of Minn. Stat. § 325D.44(1)(5);

b. Representing that goods and services are of a particular standard or quality when they are of another, in violation of Minn. Stat. § 325D.44(1)(7);

c. Advertising goods and services with intent not to sell them as advertised, in violation of Minn. Stat. § 325D.44(1)(9); and

d. Engaging in other conduct which similarly creates a likelihood of confusion or misunderstanding, in violation of Minn. Stat. § 325D.44(1)(13).

884. Equifax's deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Minnesota Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and Minnesota Subclass members'

Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Minnesota Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Minnesota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

885. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data

security and ability to protect the confidentiality of consumers' Personal Information.

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

887. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Minnesota Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the Minnesota Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

888. Equifax acted intentionally, knowingly, and maliciously to violate Minnesota's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Minnesota Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

889. As a direct and proximate result of Equifax's deceptive trade practices, Plaintiff and Minnesota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

890. Plaintiff and Minnesota Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE MISSISSIPPI SUBCLASS

COUNT 54

MISSISSIPPI CONSUMER PROTECTION ACT, Miss. Code §§ 75-24-1, *et seq.*

891. The Mississippi Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Mississippi Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

892. Equifax is a "person," as defined by Miss. Code § 75-24-3.

893. Equifax advertised, offered, or sold goods or services in Mississippi and engaged in trade or commerce directly or indirectly affecting the people of Mississippi, as defined by Miss. Code § 75-24-3.

894. Plaintiff has complied with all pre-conditions for bringing a private action under Miss. Code § 75-24-15.

895. Equifax engaged in unfair and deceptive trade acts or practices, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Mississippi Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Mississippi Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and Mississippi Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Mississippi Subclass members' Personal

Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Mississippi Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Mississippi Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

896. The above-described conduct violated Miss. Code Ann. § 75-24-5(2), including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have;

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

c. Advertising goods or services with intent not to sell them as advertised.

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

898. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

899. 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 serve as trusted linchpins of the financial system and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Mississippi Subclass. Equifax accepted the

responsibility of being a "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, Plaintiff and the Mississippi Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

900. Equifax had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the Personal Information in its possession, and the generally accepted professional standards in the credit reporting industry, and the position of trust described in the immediately-preceding paragraph. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Mississippi Subclass—and Equifax, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Equifax. Equifax's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Mississippi Subclass that contradicted these representations.

901. Equifax acted intentionally, knowingly, and maliciously to violate Mississippi's Consumer Protection Act, and recklessly disregarded Plaintiff and Mississippi Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

902. As a direct and proximate result of Equifax's unfair and deceptive acts or practices and Plaintiff and Mississippi Subclass members' purchase of goods or services primarily for personal, family, or household purposes, Plaintiff and Mississippi Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

903. Equifax's violations present a continuing risk to Plaintiff and Mississippi Subclass members as well as to the general public.

904. Plaintiff and Mississippi Subclass members seek seek all monetary and non-monetary relief allowed by law, including actual damages, restitution and other relief under Miss. Code § 75-24-11, injunctive relief, punitive damages, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE MISSOURI SUBCLASS

COUNT 55

MISSOURI MERCHANDISE PRACTICES ACT, Mo. Rev. Stat. §§ 407.010, *et seq.*

905. The Missouri Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Missouri Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

906. Equifax is a "person" as defined by Mo. Rev. Stat. § 407.010(5).

907. Equifax advertised, offered, or sold goods or services in Missouri and engaged in trade or commerce directly or indirectly affecting the people of Missouri, as defined by Mo. Rev. Stat. § 407.010(4), (6) and (7).

908. Plaintiff and Missouri Subclass members purchased or leased goods or services primarily for personal, family, or household purposes.

909. Equifax engaged in unlawful, unfair, and deceptive acts and practices, in connection with the sale or advertisement of merchandise in trade or commerce, in violation of Mo. Rev. Stat. § 407.020(1), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Missouri Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Missouri Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and Missouri Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Missouri Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Missouri Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Missouri Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

910. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

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

912. Equifax acted intentionally, knowingly, and maliciously to violate Missouri's Merchandise Practices Act, and recklessly disregarded Plaintiff and Missouri Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

913. As a direct and proximate result of Equifax's unlawful, unfair, and deceptive acts and practices, Plaintiff and Missouri Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

914. Plaintiff and Missouri Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, punitive damages, attorneys' fees and costs, injunctive relief, and any other appropriate relief.

CLAIMS ON BEHALF OF THE MONTANA SUBCLASS

COUNT 56

COMPUTER SECURITY BREACH LAW, Mont. Code Ann. §§ 30-14-1704(1), *et seq.*

915. The Montana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Montana Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

916. Equifax is a business that owns or licenses computerized data that includes Personal Information as defined by Mont. Code Ann. § 30-14-1704(4)(b). Equifax also maintains computerized data that includes Personal Information which Equifax does not own. Accordingly, it is subject to Mont. Code Ann. § 30-14-1704(1) and (2).

917. Plaintiff's and Montana Subclass members' Personal Information (*e.g.* Social Security numbers) includes Personal Information covered by Mont. Code Ann. § 30-14-1704(4)(b).

918. Equifax is required to give immediate notice of a breach of security of a data system to owners of Personal Information which Equifax does not own, including Plaintiff and Montana Subclass members, pursuant to Mont. Code Ann. § 30-14-1704(2).

919. Equifax is required to accurately notify Plaintiff and Montana Subclass members if it discovers a security breach, or receives notice of a security breach which may have compromised Personal Information which Equifax owns or licenses, without unreasonable delay under Mont. Code Ann. § 30-14-1704(1).

920. Because Equifax was aware of a security breach, Equifax had an obligation to disclose the data breach as mandated by Mont. Code Ann. § 30-14-1704(1) and (2).

921. Pursuant to Mont. Code Ann. § 30-14-1705, violations of Mont. Code Ann. § 30-14-1704 are unlawful practices under Mont. Code Ann. § 30-14-103, Montana's Consumer Protection Act.

922. As a direct and proximate result of Equifax's violations of Mont. Code Ann. § 30-14-1704(1) and (2), Plaintiff and Montana Subclass members suffered damages, as described above.

923. Plaintiff and Montana Subclass members seek relief under Mont. Code Ann. § 30-14-133, including actual damages and injunctive relief.

COUNT 57

MONTANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION ACT, M.C.A. §§ 30-14-101, *et seq.*

924. The Montana Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Montana Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

925. Equifax is a "person" as defined by MCA § 30-14-102(6).

926. Plaintiff and Montana Subclass members are "consumers" as defined by MCA§ 30-14-102(1).

927. Equifax advertised, offered, or sold goods or services in Montana and engaged in trade or commerce directly or indirectly affecting the people of Montana, as defined by MCA § 30-14-102(8).

928. Equifax engaged in unfair and deceptive acts and practices in the conduct of trade or commerce, in violation MCA § 30-14-103, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Montana Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Montana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and Montana Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Montana Subclass members' Personal Information, including duties imposed by the FTC Act, 15

U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Montana Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Montana Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

929. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

930. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Montana Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the Montana Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

931. Equifax's acts described above are unfair and offend public policy; they are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers.

932. Equifax acted intentionally, knowingly, and maliciously to violate Montana's Unfair Trade Practices and Consumer Protection Act, and recklessly disregarded Plaintiff and Montana Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

933. As a direct and proximate result of Equifax's unfair methods of competition and unfair and deceptive acts and practices in the conduct of trade or commerce, Plaintiff and Montana Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

934. Plaintiff and Montana Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of (a) actual damages or (b) statutory damages of $500, treble damages, restitution, attorneys' fees and costs, injunctive relief, and other relief that the Court deems appropriate.

CLAIMS ON BEHALF OF THE NEBRASKA SUBCLASS

COUNT 58

NEBRASKA CONSUMER PROTECTION ACT, Neb. Rev. Stat. §§ 59-1601, *et seq.*

935. The Nebraska Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Nebraska Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

936. Equifax and Nebraska Subclass members are each a "person" as defined by Neb. Rev. Stat. § 59-1601(1).

937. Equifax advertised, offered, or sold goods or services in Nebraska and engaged in trade or commerce directly or indirectly affecting the people of Nebraska, as defined by Neb. Rev. Stat. § 59-1601.

938. Equifax engaged in unfair and deceptive acts and practices in conducting trade and commerce, in violation of Neb. Rev. Stat. § 59-1602, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Nebraska Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska

Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and Nebraska Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Nebraska Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties

pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

939. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

940. As a direct and proximate result of Equifax's unfair and deceptive acts and practices, Plaintiff and Nebraska Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

941. Equifax's unfair and deceptive acts and practices complained of herein affected the public interest, including the large percentage of Nebraskans affected by the Equifax Data Breach.

942. Plaintiff and Nebraska Subclass members seek seek all monetary and non-monetary relief allowed by law, including injunctive relief, the greater of either (1) actual damages or (2) $1,000, civil penalties, and reasonable attorneys' fees and costs.

COUNT 59

NEBRASKA UNIFORM DECEPTIVE TRADE PRACTICES ACT, Neb. Rev. Stat. §§ 87-301, *et seq.*

943. The Nebraska Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Nebraska Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

944. Equifax and Nebraska Subclass members are "persons" as defined by Neb. Rev. Stat. § 87-301(19).

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

946. Equifax engaged in deceptive trade practices in the course of its business, in violation of Neb. Rev. Stat. §§ 87-302(a)(5), (8), and (10), including:

a. Represented that goods and services have characteristics, uses, benefits, or qualities that they do not have;

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

c. Advertised its goods and services with intent not to sell them as advertised and in a manner calculated or tending to mislead or deceive.

947. Equifax's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Nebraska Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C.

§ 1681e, 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 the privacy and confidentiality of Plaintiff and Nebraska Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Nebraska Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nebraska Subclass members' Personal Information, including duties

imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

948. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

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

950. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Nebraska Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the Nebraska Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

951. Equifax acted intentionally, knowingly, and maliciously to violate Nebraska's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Nebraska Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

952. As a direct and proximate result of Equifax's deceptive trade practices, Plaintiff and Nebraska Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

953. Equifax's deceptive trade practices complained of herein affected consumers at large, including the large percentage of Nebraskans affected by the Equifax Data Breach.

954. Plaintiff and Nebraska Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, civil penalties, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NEVADA SUBCLASS

COUNT 60

NEVADA DECEPTIVE TRADE PRACTICES ACT, Nev. Rev. Stat. Ann. §§ 598.0903, *et seq.*

955. The Nevada Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Nevada Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

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

957. Equifax engaged in deceptive trade practices in the course of its business or occupation, in violation of Nev. Rev. Stat. §§ 598.0915 and 598.0923, including:

a. Knowingly making a false representation as to the characteristics, uses, and benefits of goods or services for sale in violation of Nev. Rev. Stat. § 598.0915(5);

b. Representing that goods or services for sale are of a particular standard, quality, or grade when Equifax knew or should have known that they are of another standard, quality, or grade in violation of Nev. Rev. Stat. § 598.0915(7);

c. Advertising goods or services with intent not to sell them as advertised in violation of Nev. Rev. Stat § 598.0915(9);

d. Failing to disclose a material fact in connection with the sale of goods or services in violation of Nev. Rev. Stat. § 598.0923(A)(2); and

e. Violating state and federal statutes or regulations relating to the sale of goods or services in violation of Nev. Rev. Stat. § 598.0923(A)(3).

958. Equifax's deceptive trade practices in the course of its business or occupation include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Nevada Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nevada Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Nevada's data security statute, Nev. Rev. Stat. § 603A.210, which was a direct and proximate cause of the Equifax data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Nevada Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Nevada Subclass members' Personal Information,

including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*; and Nevada's data security statute, Nev. Rev. Stat. § 603A.210;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Nevada Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Nevada's data security statute, Nev. Rev. Stat. § 603A.210.

959. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

960. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Nevada Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the Nevada Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

961. Equifax acted intentionally, knowingly, and maliciously to violate Nevada's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Nevada Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

962. As a direct and proximate result of Equifax's deceptive trade practices, Plaintiff and Nevada Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

963. Plaintiff and Nevada Subclass members seek seek all monetary and non-monetary relief allowed by law, including damages, punitive damages, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NEW HAMPSHIRE SUBCLASS

COUNT 61

NOTICE OF SECURITY BREACH, N.H. Rev. Stat. Ann. §§ 359-C:20(I)(A), *et seq.*

964. The New Hampshire Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Hampshire Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

965. Equifax is a business that owns or licenses computerized data that includes Personal Information as defined by N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

966. Plaintiff's and New Hampshire Subclass members' Personal Information (*e.g.*, Social Security numbers) includes Personal Information as covered under N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

967. Equifax is required to accurately notify Plaintiff and New Hampshire Subclass members if Equifax becomes aware of a breach of its data security system in which misuse of Personal Information has occurred or is reasonably likely to occur, as soon as possible under N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

968. Because Equifax was aware of a security breach in which misuse of Personal Information has occurred or is reasonably likely to occur, Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

969. By failing to disclose the Equifax data breach in a timely and accurate manner, Equifax violated N.H. Rev. Stat. Ann. § 359-C:20(I)(a).

970. As a direct and proximate result of Equifax's violations of N.H. Rev. Stat. Ann. § 359-C:20(I)(a), Plaintiff and New Hampshire Subclass members suffered damages, as described above.

971. Plaintiff and New Hampshire Subclass members seek relief under N.H. Rev. Stat. Ann. § 359-C:21(I), including actual damages and injunctive relief.

COUNT 62

NEW HAMPSHIRE CONSUMER PROTECTION ACT, N.H.R.S.A. §§ 358-A, *et seq.*

972. The New Hampshire Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Hampshire Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

973. Equifax is a "person" under the New Hampshire Consumer Protection.

974. Equifax advertised, offered, or sold goods or services in New Hampshire and engaged in trade or commerce directly or indirectly affecting the people of New Hampshire, as defined by N.H.R.S.A. § 358-A:1.

975. Equifax engaged in unfair and deceptive acts or practices in the ordinary conduct of its trade or business, in violation of N.H.R.S.A. § 358-A:2, including:

a. Representing that its goods or services have characteristics, uses, or benefits that they do not have in violation of N.H.R.S.A. § 358-A:2.V;

b. Representing that its goods or services are of a particular standard or quality if they are of another in violation of N.H.R.S.A. § 358-A:2.VII; and

c. Advertising its goods or services with intent not to sell them as advertised in violation of N.H.R.S.A. § 358-A:2.IX.

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

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and New Hampshire Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Hampshire Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and New Hampshire Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Hampshire Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and New Hampshire Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Hampshire Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

977. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

978. Equifax acted intentionally, knowingly, and maliciously to violate New Hampshire's Consumer Protection Act, and recklessly disregarded Plaintiff and New Hampshire Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate. Equifax's acts and practices went beyond the realm of strictly private transactions.

979. As a direct and proximate result of Equifax's unfair and deceptive acts and practices, Plaintiff and New Hampshire Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

980. Plaintiff and New Hampshire Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, punitive

damages, equitable relief (including injunctive relief), restitution, civil penalties, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NEW JERSEY SUBCLASS

COUNT 63

NEW JERSEY CUSTOMER SECURITY BREACH DISCLOSURE ACT, N.J. Stat. Ann. §§ 56:8-163, *et seq.*

981. The New Jersey Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Jersey Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

982. Equifax is a business that compiles or maintains computerized records that include Personal Information on behalf of another business under N.J. Stat. Ann. § 56:8-163(b).

983. Plaintiff's and New Jersey Subclass members' Personal Information (including names, addresses, and Social Security numbers) includes Personal Information covered under N.J. Stat. Ann. §§ 56:8-163, *et seq.*

984. Under N.J. Stat. Ann. § 56:8-163(b), "[a]ny business . . . that compiles or maintains computerized records that include Personal Information on behalf of another business or public entity shall notify that business or public entity, who shall notify its New Jersey customers . . . of any breach of security of the

computerized records immediately following discovery, if the Personal Information was, or is reasonably believed to have been, accessed by an unauthorized person."

985. Because Equifax discovered a breach of its security system in which Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Personal Information was not secured, Equifax had an obligation to disclose the Equifax data breach in a timely and accurate fashion as mandated under N.J. Stat. Ann. §§ 56:8-163, *et seq.*

986. By failing to disclose the Equifax data breach in a timely and accurate manner, Equifax violated N.J. Stat. Ann. § 56:8-163(b).

987. As a direct and proximate result of Equifax's violations of N.J. Stat. Ann. § 56:8-163(b), Plaintiff and New Jersey Subclass members suffered the damages described above.

988. Plaintiff and New Jersey Subclass members seek relief under N.J. Stat. Ann. § 56:8-19, including treble damages, attorneys' fees and costs, and injunctive relief.

COUNT 64

NEW JERSEY CONSUMER FRAUD ACT, N.J. Stat. Ann. §§ 56:8-1, *et seq.*

989. The New Jersey Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Jersey Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

990. Equifax is a "person," as defined by N.J. Stat. Ann. § 56:8-1(d).

991. Equifax sells "merchandise," as defined by N.J. Stat. Ann. § 56:8-1(c) & (e).

992. The New Jersey Consumer Fraud Act, N.J. Stat. §§ 56:8-1, *et seq.*, prohibits unconscionable commercial practices, deception, fraud, false pretense, false promise, misrepresentation, as well as the knowing concealment, suppression, or omission of any material fact with the intent that others rely on the concealment, omission, or fact, in connection with the sale or advertisement of any merchandise.

993. Equifax's unconscionable and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and New Jersey Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Jersey Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and New Jersey Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Jersey Subclass members' Personal

Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Jersey Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

994. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

995. Equifax intended to mislead Plaintiff and New Jersey Subclass members and induce them to rely on its misrepresentations and omissions.

996. Equifax acted intentionally, knowingly, and maliciously to violate New Jersey's Consumer Fraud Act, and recklessly disregarded Plaintiff and New Jersey Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

997. As a direct and proximate result of Equifax's unconscionable and deceptive practices, Plaintiff and New Jersey Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

998. Plaintiff and New Jersey Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual damages, treble damages, restitution, and attorneys' fees, filing fees, and costs.

CLAIMS ON BEHALF OF THE NEW MEXICO SUBCLASS

COUNT 65

NEW MEXICO UNFAIR PRACTICES ACT, N.M. Stat. Ann. §§ 57-12-2, *et seq.*

999. The New Mexico Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New Mexico Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1000. Equifax is a "person" as meant by N.M. Stat. Ann. § 57-12-2.

1001. Equifax was engaged in "trade" and "commerce" as meant by N.M. Stat. Ann. § 57-12-2(C) when engaging in the conduct alleged.

1002. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2, *et seq.*, prohibits both unfair or deceptive trade practices and unconscionable trade practices in the conduct of any trade or commerce.

1003. Equifax engaged in unconscionable, 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);

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);

c. Knowingly using exaggeration, innuendo, or ambiguity as to a material fact or failing to state a material fact where doing so deceives or tends to deceive in violation of N.M. Stat. Ann. § 57-12-2(D)(14);

d. Taking advantage of the lack of knowledge, experience, or capacity of its consumers to a grossly unfair degree to Plaintiff's and the New Mexico Subclass' detriment in violation of N.M. Stat. Ann. § 57-2-12(E)(1); and

e. Performing these acts and practices in a way that results in a gross disparity between the value received by Plaintiff and the New Mexico Subclass and the price paid, to their detriment, in violation of N.M. Stat. § 57-2-12(E)(2).

1004. Equifax's unfair, deceptive, and unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and New Mexico Subclass

members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Mexico Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and New Mexico statutes requiring protections for social security numbers, N.M. Stat. § 57-12B-3(D), and mandating reasonable data security, N.M. Stat. § 57-12C-4, which was a direct and proximate cause of the Equifax data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and New Mexico Subclass members'

Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Mexico Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and New Mexico statutes requiring protections for social security numbers, N.M. Stat. § 57-12B-3(D), and mandating reasonable data security, N.M. Stat. § 57-12C-4;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and New Mexico Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New Mexico Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15

U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and New Mexico statutes requiring protections for social security numbers, N.M. Stat. § 57-12B-3(D), and mandating reasonable data security, N.M. Stat. § 57-12C-4.

1005. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

1006. Equifax intended to mislead Plaintiff and New Mexico Subclass members and induce them to rely on its misrepresentations and omissions.

1007. Equifax acted intentionally, knowingly, and maliciously to violate New Mexico's Unfair Practices Act, and recklessly disregarded Plaintiff and New Mexico Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1008. 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, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for

fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1009. 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.

CLAIMS ON BEHALF OF THE NEW YORK SUBCLASS

COUNT 66

INFORMATION SECURITY BREACH AND NOTIFICATION ACT, N.Y. Gen. Bus. Law § 899-aa

1010. The New York Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New York Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1011. Equifax is a business that owns or licenses computerized data that includes Personal Information as defined by N.Y. Gen. Bus. Law § 899-aa(1)(a). Equifax also maintains computerized data that includes Private Information which Equifax does not own. Accordingly, it is subject to N.Y. Gen. Bus. Law §§ 899-aa(2) and (3).

1012. Plaintiff's and New York Subclass members' Private Information (*e.g.* Social Security numbers) includes Private Information covered by N.Y. Gen. Bus. Law § 899-aa(1)(b).

1013. Equifax is required to give immediate notice of a breach of security of a data system to owners of Personal Information which Equifax does not own, including Plaintiff and New York Subclass members, pursuant to N.Y. Gen. Bus. Law § 899-aa(3).

1014. Equifax is required to accurately notify Plaintiff and Montana Subclass members if it discovers a security breach, or receives notice of a security breach which may have compromised Personal Information which Equifax owns or licenses, in the most expedient time possible and without unreasonable delay under N.Y. Gen. Bus. Law § 899-aa(2).

1015. By failing to disclose the Equifax data breach in a timely and accurate manner, Equifax violated N.Y. Gen. Bus. Law §§ 899-aa(2) and (3).

1016. As a direct and proximate result of Equifax's violations of N.Y. Gen. Bus. Law §§ 899-aa(2) and (3), Plaintiff and New York Subclass members suffered damages, as described above.

1017. Plaintiff and New York Subclass members seek relief under N.Y. Gen. Bus. Law § 899-aa(6)(b), including actual damages and injunctive relief.

COUNT 67

NEW YORK GENERAL BUSINESS LAW, N.Y. Gen. Bus. Law §§ 349, *et seq.*

1018. The New York Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the New York Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1019. Equifax engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and New York Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New York

Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and New York Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New York Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and New York Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties

pertaining to the security and privacy of Plaintiff and Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

1020. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

1021. Equifax acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregarded Plaintiff and New York Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1022. 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, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1023. 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.

1024. The above deceptive and unlawful practices and acts by Equifax caused substantial injury to Plaintiff and New York Subclass members that they could not reasonably avoid.

1025. Plaintiff and New York Subclass members seek 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.

CLAIMS ON BEHALF OF THE NORTH CAROLINA SUBCLASS

COUNT 68

NORTH CAROLINA IDENTITY THEFT PROTECTION ACT, N.C. Gen. Stat. §§ 75-60, *et seq.*

1026. The North Carolina Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the North Carolina Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1027. Equifax is a business that owns or licenses computerized data that includes Personal Information as defined by N.C. Gen. Stat. § 75-61(1).

1028. Plaintiff and North Carolina Subclass members are "consumers" as defined by N.C. Gen. Stat. § 75-61(2).

1029. Equifax is required to accurately notify Plaintiff and North Carolina Subclass members if it discovers a security breach, or receives notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), without unreasonable delay under N.C. Gen. Stat. § 75-65.

1030. Plaintiff's and North Carolina Subclass members' Personal Information includes Personal Information as covered under N.C. Gen. Stat. § 75-61(10).

1031. Because Equifax discovered a security breach and had notice of a security breach (where unencrypted and unredacted Personal Information was accessed or acquired by unauthorized persons), Equifax had an obligation to disclose the Equifax data breach in a timely and accurate fashion as mandated by N.C. Gen. Stat. § 75-65.

1032. By failing to disclose the Equifax data breach in a timely and accurate manner, Equifax violated N.C. Gen. Stat. § 75-65.

1033. A violation of N.C. Gen. Stat. § 75-65 is an unlawful trade practice under N.C. Gen. Stat. Art. 2A § 75-1.1.

1034. As a direct and proximate result of Equifax's violations of N.C. Gen. Stat. § 75-65, Plaintiff and North Carolina Subclass members suffered damages, as described above.

1035. Plaintiff and North Carolina Subclass members seek relief under N.C. Gen. Stat. §§ 75-16 and 16.1, including treble damages and attorney's fees.

COUNT 69

NORTH CAROLINA UNFAIR TRADE PRACTICES ACT, N.C. Gen. Stat. Ann. §§ 75-1.1, *et seq.*

1036. The North Carolina Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the North Carolina Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1037. Equifax advertised, offered, or sold goods or services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

1038. Equifax engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of N.C. Gen. Stat. Ann. § 75-1.1, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and North Carolina Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and North Carolina Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Carolina Subclass members' Personal

Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and North Carolina Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

1039. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

1040. Equifax intended to mislead Plaintiff and North Carolina Subclass members and induce them to rely on its misrepresentations and omissions.

1041. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the North Carolina Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the North Carolina Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

1042. Equifax acted intentionally, knowingly, and maliciously to violate North Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff and North Carolina Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1043. As a direct and proximate result of Equifax's unfair and deceptive acts and practices, Plaintiff and North Carolina Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1044. Equifax's conduct as alleged herein was continuous, such that after the first violations of the provisions pled herein, each week that the violations continued constitute separate offenses pursuant to N.C. Gen. Stat. Ann. § 75-8.

1045. Plaintiff and North Carolina Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE NORTH DAKOTA SUBCLASS

COUNT 70

NOTICE OF SECURITY BREACH FOR PERSONAL INFORMATION, N.D. Cent. Code §§ 51-30-02, *et seq.*

1046. The North Dakota Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the North Dakota Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1047. Equifax is a business that owns or licenses computerized data that includes Personal Information as defined by N.D. Cent. Code § 51-30-01(4). Equifax also maintains computerized data that includes Personal Information which Equifax does not own. Accordingly, it is subject to N.D. Cent. Code §§ 51-30-02 and 03.

1048. Plaintiff's and North Dakota Subclass members' Personal Information (*e.g.* Social Security numbers) includes Personal Information covered by N.D. Cent. Code § 51-30-01(4).

1049. Equifax is required to give immediate notice of a breach of security of a data system to owners of Personal Information which Equifax does not own, including Plaintiff and North Dakota Subclass members, pursuant to N.D. Cent. Code § 51-30-03.

1050. Equifax is required to accurately notify Plaintiff and North Dakota Subclass members if it discovers a security breach, or receives notice of a security breach which may have compromised Personal Information which Equifax owns or licenses, in the most expedient time possible and without unreasonable delay under N.D. Cent. Code § 51-30-02.

1051. Because Equifax was aware of a security breach, Equifax had an obligation to disclose the data breach as mandated by N.D. Cent. Code §§ 51-30-02 and 51-30-03.

1052. Pursuant to N.D. Cent. Code § 51-30-07, violations of N.D. Cent. Code §§ 51-30-02 and 51-30-03 are unlawful sales or advertising practices which violate chapter 51-15 of the North Dakota Century Code.

1053. As a direct and proximate result of Equifax's violations of N.D. Cent. Code §§ 51-30-02 and 51-30-03, Plaintiff and North Dakota Subclass members suffered damages, as described above.

1054. Plaintiff and North Dakota Subclass members seek relief under N.D. Cent. Code §§ 51-15-01 *et seq*., including actual damages and injunctive relief.

COUNT 71

NORTH DAKOTA UNLAWFUL SALES OR ADVERTISING ACT, N.D. Cent. Code §§ 51-15-01, *et seq.*

1055. The North Dakota Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the North Dakota Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1056. Equifax, Plaintiff, and each member of the North Dakota Subclass is a "person," as defined by N.D. Cent. Code § 51-15-01(4).

1057. Equifax sells and advertises "merchandise," as defined by N.D. Cent. Code § 51-15-01(3) and (5).

1058. Equifax advertised, offered, or sold goods or services in North Dakota and engaged in trade or commerce directly or indirectly affecting the people of North Dakota.

1059. Equifax engaged in deceptive, false, fraudulent, misrepresentative, unconscionable, and substantially injurious acts and practices in connection with the sale and advertisement of merchandise, in violation of N.D. Cent. Code § 51-15-01, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and North Dakota Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Dakota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and North Dakota Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Dakota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and North Dakota Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Dakota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

1060. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

1061. The Equifax's above-described acts and practices caused substantial injury to Plaintiff and North Dakota Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

1062. Equifax intended to mislead Plaintiff and North Dakota Subclass members and induce them to rely on its misrepresentations and omissions.

1063. Equifax acted intentionally, knowingly, and maliciously to violate North Dakota's Unlawful Sales or Advertising Law, and recklessly disregarded Plaintiff and North Dakota Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1064. As a direct and proximate result of Equifax's deceptive, unconscionable, and substantially injurious practices, Plaintiff and North Dakota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1065. Plaintiff and North Dakota Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, damages, restitution, treble damages, civil penalties, and attorneys' fees, costs, and disbursements.

CLAIMS ON BEHALF OF THE OHIO SUBCLASS

COUNT 72

OHIO CONSUMER SALES PRACTICES ACT, Ohio Rev. Code §§ 1345.01, *et seq.*

1066. The Ohio Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Ohio Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1067. Plaintiff and Ohio Subclass members are "persons," as defined by Ohio Rev. Code § 1345.01(B).

1068. Equifax was a "supplier" engaged in "consumer transactions," as defined by Ohio Rev. Code §§ 1345.01(A) & (C).

1069. Equifax advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

1070. Equifax engaged in unfair and deceptive acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code §§ 1345.02, including:

a. Equifax represented that its goods, services, and intangibles had performance characteristics, uses, and benefits that it did not have, in violation of Ohio Rev. Code § 1345.02(B)(1); and

b. Equifax represented that its goods, services, and intangibles were of a particular standard or quality when they were not, in violation of Ohio Rev. Code § 1345(B)(2).

1071. Equifax engaged in unconscionable acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code Ann. § 1345.03, including:

a. Knowingly taking advantage of the inability of Plaintiff and the Ohio Subclass to reasonably protect their interest because of their ignorance of the issues discussed herein (Ohio Rev. Code Ann. § 1345.03(B)(1)); and

b. Requiring Plaintiff and the Ohio Subclass to enter into a consumer transaction on terms that Equifax knew were substantially one-sided in favor of Equifax (Ohio Rev. Code Ann. § 1345.03(B)(5)).

1072. Equifax's unfair, deceptive, and unconscionable acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Ohio Subclass

members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Ohio Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information,

including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Ohio Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

1073. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

1074. Equifax intended to mislead Plaintiff and Ohio Subclass members and induce them to rely on its misrepresentations and omissions.

1075. Equifax acted intentionally, knowingly, and maliciously to violate Ohio's Consumer Sales Practices Act, and recklessly disregarded Plaintiff and Ohio Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1076. Equifax's unfair, deceptive, and unconscionable acts and practices complained of herein affected the public interest, including the millions of Ohioans affected by the Equifax Data Breach.

1077. As a direct and proximate result of Equifax's unfair, deceptive, and unconscionable acts and practices, Plaintiff and Ohio Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1078. Plaintiff and the Ohio Subclass members seek all monetary and non-monetary relief allowed by law, including declaratory and injunctive relief, the greater of actual and treble damages or statutory damages, attorneys' fees and costs, and any other appropriate relief.

COUNT 73

OHIO DECEPTIVE TRADE PRACTICES ACT, Ohio Rev. Code §§ 4165.01, *et seq.*

1079. The Ohio Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Ohio Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1080. Equifax, Plaintiff, and Ohio Subclass members are a "person," as defined by Ohio Rev. Code § 4165.01(D).

1081. Equifax advertised, offered, or sold goods or services in Ohio and engaged in trade or commerce directly or indirectly affecting the people of Ohio.

1082. Equifax engaged in deceptive trade practices in the course of its business and vocation, in violation of Ohio Rev. Code § 4165.02, including:

a. Representing that its goods and services have characteristics, uses, benefits, or qualities that they do not have, in violation of Ohio Rev. Code § 4165.02(A)(7);

b. Representing that its goods and services are of a particular standard or quality when they are of another, in violation of Ohio Rev. Code § 4165.02(A)(9); and

c. Advertising its goods and services with intent not to sell them as advertise, in violation of Ohio Rev. Code § 4165.02(A)(11).

1083. Equifax's deceptive trade practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Ohio Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Ohio Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Ohio Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Ohio Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

1084. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

1085. Equifax intended to mislead Plaintiff and Ohio Subclass members and induce them to rely on its misrepresentations and omissions.

1086. Equifax acted intentionally, knowingly, and maliciously to violate Ohio's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Ohio Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1087. As a direct and proximate result of Equifax's deceptive trade practices, Plaintiff and Ohio Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1088. Plaintiff and Ohio Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, attorneys' fees, and any other relief that is just and proper.

CLAIMS ON BEHALF OF THE OKLAHOMA SUBCLASS

COUNT 74

OKLAHOMA CONSUMER PROTECTION ACT, Okla. Stat. Tit. 15, §§ 751, *et seq.*

1089. The Oklahoma Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Oklahoma Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1090. Equifax is a "person," as meant by Okla. Stat. tit. 15, § 752(1).

1091. Equifax's advertisements, offers of sales, sales, and distribution of goods, services, and other things of value constituted "consumer transactions" as meant by Okla. Stat. tit. 15, § 752(2).

1092. Equifax, in the course of its business, engaged in unlawful practices in violation of Okla. Stat. tit. 15, § 753, including the following:

a. Making false representations, knowingly or with reason to know, as to the characteristics, uses, and benefits of the subjects of its consumer transactions, in violation of Okla. Stat. tit. 15, § 753(5);

b. Representing, knowingly or with reason to know, that the subjects of its consumer transactions were of a particular

standard when they were of another, in violation of Okla. Stat. tit 15, § 753(7);

c. Advertising, knowingly or with reason to know, the subjects of its consumer transactions with intent not to sell as advertised, in violation of Okla. Stat. tit 15, § 753 (8);

d. Committing unfair trade practices that offend established public policy and was immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers as defined by section 752(14), in violation of Okla. Stat. tit. 15, § 753(20); and

e. Committing deceptive trade practices that deceived or could reasonably be expected to deceive or mislead a person to the detriment of that person as defined by section 752(13), in violation of Okla. Stat. tit. 15, § 753(20).

1093. Equifax's unlawful practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Oklahoma Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oklahoma Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Oklahoma Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oklahoma Subclass members' Personal Information, including duties imposed by the FTC Act, 15

U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Oklahoma Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oklahoma Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

1094. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

1095. Equifax intended to mislead Plaintiff and Oklahoma Subclass members and induce them to rely on its misrepresentations and omissions.

1096. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Oklahoma Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the Oklahoma Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

1097. The above unlawful practices and acts by Equifax were immoral, unethical, oppressive, unscrupulous, and substantially injurious. These acts caused substantial injury to Plaintiff and Oklahoma Subclass members.

1098. Equifax acted intentionally, knowingly, and maliciously to violate Oklahoma's Consumer Protection Act, and recklessly disregarded Plaintiff and Oklahoma Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1099. As a direct and proximate result of Equifax's unlawful practices, Plaintiff and Oklahoma Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1100. Plaintiff and Oklahoma Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, civil penalties, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE OREGON SUBCLASS

COUNT 75

OREGON CONSUMER IDENTITY THEFT PROTECTION ACT, Or. Rev. Stat. §§ 646A.604(1), *et seq.*

1101. The Oregon Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Oregon Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1102. Equifax is a business that maintains records which contain Personal Information, within the meaning of Or. Rev. Stat. § 646A.622(1), about Plaintiff and Oregon Subclass members.

1103. Pursuant to Or. Rev. Stat. § 646A.622(1), a business "that maintains records which contain Personal Information" of an Oregon resident "shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure."

1104. Equifax violated Or. Rev. Stat. § 646A.622(1) by failing to implement reasonable measures to protect Plaintiff's and Oregon Subclass members' Personal Information.

1105. Equifax is a business that owns, maintains, or otherwise possesses data that includes consumers Personal Information as defined by Or. Rev. Stat. § 646A.604(1).

1106. Plaintiff's and Oregon Subclass members' Personal Information includes Personal Information as covered under Or. Rev. Stat. § 646A.604(1).

1107. Equifax is required to accurately notify Plaintiff and Oregon Subclass members if it becomes aware of a breach of its data security system in the most expeditious time possible and without unreasonable delay under Or. Rev. Stat. § 646A.604(1).

1108. Because Equifax discovered a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Or. Rev. Stat. § 646A.604(1).

1109. By failing to disclose the Equifax data breach in a timely and accurate manner, Equifax violated Or. Rev. Stat. § 646A.604(1).

1110. Pursuant to Or. Rev. Stat. § 646A.604(9), violations of Or. Rev. Stat. §§ 646A.604(1) and 646A.622(1) are unlawful practices under Or. Rev. Stat. § 646.607.

1111. As a direct and proximate result of Equifax's violations of Or. Rev. Stat. §§ 646A.604(1) and 646A.622(1), Plaintiff and Oregon Subclass members suffered damages, as described above.

1112. Plaintiff and Oregon Subclass members seek relief under Or. Rev. Stat. § 646.638, including actual damages, punitive damages, and injunctive relief.

COUNT 76

OREGON UNLAWFUL TRADE PRACTICES ACT, Or. Rev. Stat. §§ 646.608, *et seq.*

1113. The Oregon Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Oregon Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1114. Equifax is a "person," as defined by Or. Rev. Stat. § 646.605(4).

1115. Equifax engaged in the sale of "goods and services," as defined by Or. Rev. Stat. § 646.605(6)(a).

1116. Equifax sold "goods or services," as defined by Or. Rev. Stat. § 646.605(6)(a).

1117. Equifax advertised, offered, or sold goods or services in Oregon and engaged in trade or commerce directly or indirectly affecting the people of Oregon.

1118. Equifax engaged in unlawful practices in the course of its business and occupation, in violation of Or. Rev. Stat. § 646.608, included the following:

a. Representing that its goods and services have approval, characteristics, uses, benefits, and qualities that they do not have, in violation of Or. Rev. Stat. § 646.608(1)(e);

b. Representing that its goods and services are of a particular standard or quality if they are of another, in violation of Or. Rev. Stat. § 646.608(1)(g);

c. Advertising its goods or services with intent not to provide them as advertised, in violation of Or. Rev. Stat. § 646.608(1)(i); and

d. Concurrent with tender or delivery of its goods and services, failing to disclose any known material defect, in violation of Or. Rev. Stat. § 646.608(1)(t).

1119. Equifax's unlawful practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Oregon Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oregon Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§

646A.600, *et seq.*, which was a direct and proximate cause of the Equifax data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Oregon Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oregon Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Oregon Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Oregon

Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Oregon's Consumer Identity Theft Protection Act, Or. Rev. Stat. §§ 646A.600, *et seq.*

1120. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

1121. Equifax intended to mislead Plaintiff and Oregon Subclass members and induce them to rely on its misrepresentations and omissions.

1122. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Oregon Subclass. Equifax accepted the responsibility of

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

1123. Equifax acted intentionally, knowingly, and maliciously to violate Oregon's Unlawful Trade Practices Act, and recklessly disregarded Plaintiff and Oregon Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1124. As a direct and proximate result of Equifax's unlawful practices, Plaintiff and Oregon Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1125. Plaintiff and Oregon Subclass members seek all monetary and non-monetary relief allowed by law, including equitable relief, actual damages or

statutory damages of $200 per violation (whichever is greater), punitive damages, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE PENNSYLVANIA SUBCLASS

COUNT 77

PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, 73 Pa. Cons. Stat. §§ 201-2 & 201-3, *et seq.*

1126. The Pennsylvania Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Pennsylvania Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1127. Equifax is a "person", as meant by 73 Pa. Cons. Stat. § 201-2(2).

1128. Plaintiff and Pennsylvania Subclass members purchased goods and services in "trade" and "commerce," as meant by 73 Pa. Cons. Stat. § 201-2(3), primarily for personal, family, and/or household purposes.

1129. Equifax Pennsylvania engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including the following:

a. Representing that its goods and services have characteristics, uses, benefits, and qualities that they do not have (73 Pa. Stat. Ann. § 201-2(4)(v));

b. Representing that its goods and services are of a particular standard or quality if they are another (73 Pa. Stat. Ann. § 201-2(4)(vii)); and

c. Advertising its goods and services with intent not to sell them as advertised (73 Pa. Stat. Ann. § 201-2(4)(ix)).

1130. Equifax's unfair or deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Pennsylvania Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Pennsylvania Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the

FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Pennsylvania Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Pennsylvania Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Pennsylvania Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Pennsylvania Subclass members' Personal Information,

including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

1131. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

1132. Equifax intended to mislead Plaintiff and Pennsylvania Subclass members and induce them to rely on its misrepresentations and omissions.

1133. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Pennsylvania Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the Pennsylvania Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

1134. Equifax acted intentionally, knowingly, and maliciously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Pennsylvania Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1135. As a direct and proximate result of Equifax's unfair methods of competition and unfair or deceptive acts or practices and Plaintiff's and the Pennsylvania Subclass' reliance on them, Plaintiff and Pennsylvania Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1136. Plaintiff and Pennsylvania Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory

damages of $100 (whichever is greater), treble damages, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

CLAIMS ON BEHALF OF THE PUERTO RICO SUBCLASS

COUNT 78

CITIZEN INFORMATION ON DATA BANKS SECURITY ACT, P.R. Laws Ann. tit. 10, §§ 4051, *et seq.*

1137. Plaintiffs, on behalf of the Puerto Rico Subclass, repeat and allege Paragraphs 1-313, as if fully alleged herein.

1138. Equifax is the owner and custodian of databases that include Personal Information as defined by P.R. Laws Ann. tit. 10, § 4051(a), and is therefore subject to. P.R. Laws Ann. tit. 10, § 4052.

1139. Plaintiff's and Puerto Rico Subclass members' Personal Information (e.g., Social Security numbers) includes personal identifying information as covered under P.R. Laws Ann. tit. 10, § 4051(a).

1140. Equifax is required to accurately notify Plaintiff and Puerto Rico Subclass members following discovery or notification of a breach of its data security system as expeditiously as possible under P.R. Laws Ann. tit. 10, § 4052.

1141. Because Equifax discovered a breach of its data security system, Equifax had an obligation to disclose the Equifax data breach in a timely and accurate fashion as mandated by P.R. Laws Ann. tit. 10, § 4052.

1142. By failing to disclose the Equifax data breach in a timely and accurate manner, Equifax violated P.R. Laws Ann. tit. 10, § 4052.

1143. As a direct and proximate result of Equifax's violations of P.R. Laws Ann. tit. 10, § 4052, Plaintiff and Puerto Rico Subclass members suffered damages, as described above.

1144. Plaintiff and Puerto Rico Subclass members seek relief under P.R. Laws Ann. tit. 10, § 4055, including actual damages and injunctive relief.

CLAIMS ON BEHALF OF THE RHODE ISLAND SUBCLASS

COUNT 79

RHODE ISLAND DECEPTIVE TRADE PRACTICES ACT, R.I. Gen. Laws §§ 6-13.1, *et seq.*

1145. The Rhode Island Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Rhode Island Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1146. Plaintiff and Rhode Island Subclass members are each a "person," as defined by R.I. Gen. Laws § 6-13.1-1(3).

1147. Plaintiff and Rhode Island Subclass members purchased goods and services for personal, family, or household purposes.

1148. Equifax advertised, offered, or sold goods or services in Rhode Island and engaged in trade or commerce directly or indirectly affecting the people of Rhode Island, as defined by R.I. Gen. Laws § 6-13.1-1(5).

1149. Equifax engaged in unfair and deceptive acts and practices, in violation of R.I. Gen. Laws § 6-13.1-2, including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have (R.I. Gen. Laws § 6-13.1-52(6)(v));

b. Representing that its goods and services are of a particular standard or quality when they are of another (R.I. Gen. Laws § 6-13.1-52(6)(vii));

c. Advertising goods or services with intent not to sell them as advertised (R.I. Gen. Laws § 6-13.1-52(6)(ix));

d. Engaging in any other conduct that similarly creates a likelihood of confusion or misunderstanding (R.I. Gen. Laws § 6-13.1-52(6)(xii));

e. Engaging in any act or practice that is unfair or deceptive to the consumer (R.I. Gen. Laws § 6-13.1-52(6)(xiii)); and

f. Using other methods, acts, and practices that mislead or deceive members of the public in a material respect (R.I. Gen. Laws § 6-13.1-52(6)(xiv)).

1150. Equifax's unfair and deceptive acts include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Rhode Island Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Rhode Island Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen.

Laws § 11-49.3-2, which was a direct and proximate cause of the Equifax data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Rhode Island Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Rhode Island Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-2;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Rhode Island Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Rhode

Island Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and the Rhode Island Identity Theft Protection Act of 2015, R.I. Gen. Laws § 11-49.3-2.

1151. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

1152. Equifax intended to mislead Plaintiff and Rhode Island Subclass members and induce them to rely on its misrepresentations and omissions.

1153. Equifax acted intentionally, knowingly, and maliciously to violate Rhode Island's Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Rhode Island Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1154. As a direct and proximate result of Equifax's unfair and deceptive acts, Plaintiff and Rhode Island Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses

related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1155. Plaintiff and Rhode Island Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $200 per Subclass Member (whichever is greater), punitive damages, injunctive relief, other equitable relief, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE SOUTH CAROLINA SUBCLASS

COUNT 80

SOUTH CAROLINA DATA BREACH SECURITY ACT, S.C. Code Ann. §§ 39-1-90, *et seq.*

1156. The South Carolina Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the South Carolina Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1157. Equifax is a business that owns or licenses computerized data or other data that includes personal identifying information as defined by S.C. Code Ann. § 39-1-90(A).

1158. Plaintiff's and South Carolina Subclass members' Personal Information (*e.g.*, Social Security numbers) includes personal identifying information as covered under S.C. Code Ann. § 39-1-90(D)(3).

1159. Equifax is required to accurately notify Plaintiff and South Carolina Subclass members following discovery or notification of a breach of its data security system if Personal Information that was not rendered unusable through encryption, redaction, or other methods was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, in the most expedient time possible and without unreasonable delay under S.C. Code Ann. § 39-1-90(A).

1160. Because Equifax discovered a breach of its data security system in which Personal Information that was not rendered unusable through encryption, redaction, or other methods, was, or was reasonably believed to have been, acquired by an unauthorized person, creating a material risk of harm, Equifax had an obligation to disclose the Equifax data breach in a timely and accurate fashion as mandated by S.C. Code Ann. § 39-1-90(A).

1161. By failing to disclose the Equifax data breach in a timely and accurate manner, Equifax violated S.C. Code Ann. § 39-1-90(A).

1162. As a direct and proximate result of Equifax's violations of S.C. Code Ann. § 39-1-90(A), Plaintiff and South Carolina Subclass members suffered damages, as described above.

1163. Plaintiff and South Carolina Subclass members seek relief under S.C. Code Ann. § 39-1-90(G), including actual damages and injunctive relief.

COUNT 81

SOUTH CAROLINA UNFAIR TRADE PRACTICES ACT, S.C. Code Ann. §§ 39-5-10, *et seq.*

1164. The South Carolina Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the South Carolina Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1165. Equifax is a "person," as defined by S.C. Code Ann. § 39-5-10(a).

1166. South Carolina's Unfair Trade Practices Act (SC UTPA) prohibits "unfair or deceptive acts or practices in the conduct of any trade or commerce." S.C. Code Ann. § 39-5-20.

1167. Equifax advertised, offered, or sold goods or services in South Carolina and engaged in trade or commerce directly or indirectly affecting the people of South Carolina, as defined by S.C. Code Ann. § 39-5-10(b).

1168. Equifax engaged in unfair and deceptive acts and practices, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and South Carolina Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and South Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and South Carolina Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and South Carolina Subclass members' Personal

Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and South Carolina Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and South Carolina Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

1169. Equifax's acts and practices had, and continue to have, the tendency or capacity to deceive.

1170. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

1171. Equifax intended to mislead Plaintiff and South Carolina Subclass members and induce them to rely on its misrepresentations and omissions.

1172. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the South Carolina Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the South Carolina Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

1173. Equifax had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the Personal Information in its possession, and the generally accepted professional standards in

the credit reporting industry. Such a duty is also implied by law due to the nature of the relationship between consumers—including Plaintiff and the South Carolina Subclass—and Equifax, because consumers are unable to fully protect their interests with regard to the Personal Information in Equifax's possession, and place trust and confidence in Equifax. Equifax's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the South Carolina Subclass that contradicted these representations.

1174. Equifax's business acts and practices offend an established public policy, or are immoral, unethical, or oppressive. Equifax's acts and practices offend established public policies that seek to protect consumers' Personal Information and ensure that entities entrusted with Personal Information use appropriate security measures. These public policies are reflected in laws such as the FTC Act, 15 U.S.C. § 45; FCRA, 15 U.S.C. § 1681e; the Gramm-Leach Bliley

Act, 15 U.S.C. § 6801(a); and the South Carolina Data Breach Security Act, S.C. Code § 39-1-90, *et seq.*

1175. Equifax's failure to implement and maintain reasonable security measures was immoral, unethical, or oppressive in light of Equifax's long history of inadequate data security and previous data breaches; the sensitivity and extensivity of Personal Information in its possession; its special role as a linchpin of the financial system; and its admitted duty of trustworthiness and care as an entrusted steward of data.

1176. Equifax's unfair and deceptive acts or practices adversely affected the public interest because such acts or practices have the potential for repetition; Equifax engages in such acts or practices as a general rule; and such acts or practices impact the public at large, including the 2.4 million South Carolinians impacted by the Equifax Data Breach, nearly half the state's population.

1177. Equifax's unfair and deceptive acts or practices have the potential for repetition because the same kinds of actions occurred in the past, including numerous past data breaches, thus making it likely that these acts or practices will continue to occur if left undeterred. Additionally, Equifax's policies and procedures, such as its security practices, create the potential for recurrence of the complained-of business acts and practices.

1178. Equifax's violations present a continuing risk to Plaintiff and South Carolina Subclass members as well as to the general public.

1179. Equifax intended to mislead Plaintiff and South Carolina Subclass members and induce them to rely on its misrepresentations and omissions.

1180. Equifax acted intentionally, knowingly, and maliciously to violate South Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff and South Carolina Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate. In light of this conduct, punitive damages would serve the interest of society in punishing and warning others not to engage in such conduct, and would deter Equifax and others from committing similar conduct in the future.

1181. As a direct and proximate result of Equifax's unfair and deceptive acts or practices, Plaintiff and South Carolina Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1182. Plaintiff and South Carolina Subclass members seek all monetary and non-monetary relief allowed by law, including damages for their economic losses; treble damages; punitive damages; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE SOUTH DAKOTA SUBCLASS

COUNT 82

SOUTH DAKOTA DECEPTIVE TRADE PRACTICES AND CONSUMER PROTECTION ACT, S.D. Codified Laws §§ 37-24-1, *et seq.*

1183. The South Dakota Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the South Dakota Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1184. Equifax is a "person," as defined by S.D. Codified Laws § 37-24-1(8).

1185. Equifax advertises and sells "merchandise," as defined by S.D. Codified Laws § 37-24-1(6), (7), & (13).

1186. Equifax advertised, offered, or sold goods or services in South Dakota and engaged in trade or commerce directly or indirectly affecting the people of South Dakota, as defined by S.D. Codified Laws § 37-24-1(6), (7), & (13).

1187. Equifax knowingly engaged in deceptive acts or practices, misrepresentation, concealment, suppression, or omission of material facts in

connection with the sale and advertisement of goods or services, in violation of S.D. Codified Laws § 37-24-6, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and South Dakota Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and South Dakota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and South Dakota Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and South Dakota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and South Dakota Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and South Dakota Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

1188. Equifax intended to mislead Plaintiff and South Dakota Subclass members and induce them to rely on its misrepresentations and omissions.

1189. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

1190. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the South Dakota Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the South Dakota Subclass members acted

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

1191. Equifax had a duty to disclose the above facts because members of the public, including Plaintiff and the South Dakota Subclass, repose a trust and confidence in Equifax as one of the nation's entrusted "stewards of data" and Equifax's position as one of three nationwide credit-reporting companies that serve as linchpins of the financial system. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the South Dakota Subclass, and Equifax because consumers are unable to fully protect their interests with regard to their data, and have placed trust and confidence in Equifax. Equifax's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the South Dakota Subclass that contradicted these representations.

1192. As a direct and proximate result of Equifax's deceptive acts or practices, misrepresentations, and concealment, suppression, and/or omission of material facts, Plaintiff and South Dakota Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1193. Equifax's violations present a continuing risk to Plaintiff and South Dakota Subclass members as well as to the general public.

1194. Plaintiff and South Dakota Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, injunctive relief, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE TENNESSEE SUBCLASS

COUNT 83

TENNESSEE PERSONAL CONSUMER INFORMATION RELEASE ACT, Tenn. Code Ann. §§ 47-18-2107, *et seq.*

1195. The Tennessee Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Tennessee Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1196. Equifax is a business that owns or licenses computerized data that includes Personal Information as defined by Tenn. Code Ann. § 47-18-2107(a)(2).

1197. Plaintiff's and Tennessee Subclass members' Personal Information (*e.g.*, Social Security numbers) include Personal Information as covered under Tenn. Code Ann. § 47-18- 2107(a)(3)(A).

1198. Equifax is required to accurately notify Plaintiff and Tennessee Subclass members following discovery or notification of a breach of its data security system in which unencrypted Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person, in the most expedient time possible and without unreasonable delay under Tenn. Code Ann. § 47-18-2107(b).

1199. Because Equifax discovered a breach of its security system in which unencrypted Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person, Equifax had an obligation to disclose the Equifax data breach in a timely and accurate fashion as mandated by Tenn. Code Ann. § 47-18-2107(b).

1200. By failing to disclose the Equifax data breach in a timely and accurate manner, Equifax violated Tenn. Code Ann. § 47-18-2107(b).

1201. As a direct and proximate result of Equifax's violations of Tenn. Code Ann. § 47-18-2107(b), Plaintiff and Tennessee Subclass members suffered damages, as described above.

1202. Plaintiff and Tennessee Subclass members seek relief under Tenn. Code Ann. §§ 47-18-2107(h), 47-18-2104(d), and 47-18-2104(f), including actual damages, injunctive relief, and treble damages.

COUNT 84

TENNESSEE CONSUMER PROTECTION ACT, Tenn. Code Ann. §§ 47-18-101, *et seq.*

1203. The Tennessee Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Tennessee Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1204. Equifax is a "person," as defined by Tenn. Code § 47-18-103(13).

1205. Plaintiff and Tennessee Subclass members are "consumers," as meant by Tenn. Code § 47-18-103(2).

1206. Equifax advertised and sold "goods" or "services" in "consumer transaction[s]," as defined by Tenn. Code §§ 47-18-103(7), (18) & (19).

1207. Equifax advertised, offered, or sold goods or services in Tennessee and engaged in trade or commerce directly or indirectly affecting the people of Tennessee, as defined by Tenn. Code §§ 47-18-103(7), (18) & (19). And Equifax's acts or practices affected the conduct of trade or commerce, under Tenn. Code § 47-18-104.

1208. Equifax's unfair and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Tennessee Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Tennessee Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and Tennessee Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Tennessee Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Tennessee Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

1209. Equifax intended to mislead Plaintiff and Tennessee Subclass members and induce them to rely on its misrepresentations and omissions.

1210. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

1211. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers,

including Plaintiff and the Tennessee Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the Tennessee Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

1212. Equifax had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extensivity of the Personal Information in its possession, and the generally accepted professional standards in the credit reporting industry. This duty arose because members of the public, including Plaintiff and the Tennessee Subclass, repose a trust and confidence in Equifax as one of the nation's entrusted "stewards of data" and Equifax's position as one of three nationwide credit-reporting companies that serve as linchpins of the financial system. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the Tennessee Subclass, and Equifax because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Equifax. Equifax's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Tennessee Subclass that contradicted these representations.

1213. Equifax's "unfair" acts and practices caused or were likely to cause substantial injury to consumers, which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

1214. The injury to consumers was and is substantial because it was non-trivial and non-speculative, and involved a monetary injury and/or an unwarranted risk to the safety of their Personal Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1215. Consumers could not have reasonably avoided injury because Equifax's business acts and practices unreasonably created or took advantage of an

obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Equifax created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury. Equifax's business acts and practices also took advantage of its special status as one the nation's three major credit bureaus, making it functionally impossible for consumers to obtain credit without their Personal Information being in Equifax's systems.

1216. Equifax's inadequate data security had no countervailing benefit to consumers or to competition.

1217. By misrepresenting and omitting material facts about its data security and failing to comply with its common law and statutory duties pertaining to data security (including its duties under the FTC Act; FCRA; and the GLBA), Equifax violated the following provisions of Tenn. Code § 47-18-104(b):

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;

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

c. Advertising goods or services with intent not to sell them as advertised; and

d. Representing that a consumer transaction confers or involves rights, remedies or obligations that it does not have or involve.

1218. Equifax acted intentionally, knowingly, and maliciously to violate Tennessee's Consumer Protection Act, and recklessly disregarded Plaintiff and Tennessee Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1219. As a direct and proximate result of Equifax's unfair and deceptive acts or practices, Plaintiff and Tennessee Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1220. Equifax's violations present a continuing risk to Plaintiff and Tennessee Subclass members as well as to the general public.

1221. Plaintiff and Tennessee Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, actual damages, treble

damages for each willful or knowing violation, attorneys' fees and costs, and any other relief that is necessary and proper.

CLAIMS ON BEHALF OF THE TEXAS SUBCLASS

COUNT 85

DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT, Texas Bus. & Com. Code §§ 17.41, *et seq.*

1222. The Texas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Texas Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1223. Equifax is a "person," as defined by Tex. Bus. & Com. Code § 17.45(3).

1224. Plaintiffs and the Texas Subclass members are "consumers," as defined by Tex. Bus. & Com. Code § 17.45(4).

1225. Equifax advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

1226. Equifax engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities 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. Advertising goods or services with intent not to sell them as advertised.

1227. Equifax's false, misleading, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Texas Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Texas

Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Equifax data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Texas Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Texas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Texas Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Texas Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and Texas's data security statute, Tex. Bus. & Com. Code § 521.052.

1228. Equifax intended to mislead Plaintiff and Texas Subclass members and induce them to rely on its misrepresentations and omissions.

1229. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

1230. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and

valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Texas Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the Texas Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

1231. Equifax had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extensivity of the Personal Information in its possession, and the generally accepted professional standards in the credit reporting industry. This duty arose because members of the public, including Plaintiffs and the Texas Subclass, repose a trust and confidence in Equifax as one of the nation's entrusted "stewards of data" and Equifax's position as one of three nationwide credit-reporting companies that serve as linchpins of the financial system. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiffs and the Texas Subclass, and Equifax because consumers are unable to fully protect their interests with regard to

their data, and placed trust and confidence in Equifax. Equifax's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiffs and the Texas Subclass that contradicted these representations.

1232. Equifax engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). Equifax engaged in acts or practices which, to consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

1233. Consumers, including Plaintiffs and Texas Subclass members, lacked knowledge about deficiencies in Equifax's data security because this information was known exclusively by Equifax. Consumers also lacked the ability, experience, or capacity to secure the Personal Information in Equifax's possession or to fully protect their interests with regard to their data. Plaintiffs and Texas Subclass members lack expertise in information security matters and do not have access to

Equifax's systems in order to evaluate its security controls. Equifax took advantage of its special skill and access to Personal Information to hide its inability to protect the security and confidentiality of Plaintiffs and Texas Subclass members' Personal Information.

1234. Equifax intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from Equifax's conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Equifax data breach, which resulted from Equifax's unconscionable business acts and practices, exposed Plaintiffs and Texas Subclass members to a wholly unwarranted risk to the safety of their Personal Information and the security of their identity or credit, and worked a substantial hardship on a significant and unprecedented number of consumers. Plaintiffs and Texas Subclass members cannot mitigate this unfairness because they cannot undo the data breach.

1235. Equifax acted intentionally, knowingly, and maliciously to violate Texas's Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiff and Texas Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1236. As a direct and proximate result of Equifax's unconscionable and deceptive acts or practices, Plaintiffs and Texas Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information. Equifax's unconscionable and deceptive acts or practices were a producing cause of Plaintiffs' and Texas Subclass members' injuries, ascertainable losses, economic damages, and non-economic damages, including their mental anguish.

1237. Equifax's violations present a continuing risk to Plaintiffs and Texas Subclass members as well as to the general public.

1238. Plaintiffs and the Texas Subclass seek all monetary and non-monetary relief allowed by law, including economic damages; damages for mental anguish; treble damages for each act committed intentionally or knowingly; court costs; reasonably and necessary attorneys' fees; injunctive relief; and any other relief which the court deems proper.

CLAIMS ON BEHALF OF THE UTAH SUBCLASS

COUNT 86

UTAH CONSUMER SALES PRACTICES ACT, Utah Code §§ 13-11-1, *et seq.*

1239. The Utah Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Utah Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1240. Equifax is a "person," as defined by Utah Code § 13-11-1(5).

1241. Equifax is a "supplier," as defined by Utah Code § 13-11-1(6), because it regularly solicits, engages in, or enforces "consumer transactions," as defined by Utah Code § 13-11-1(2).

1242. Equifax engaged in deceptive and unconscionable acts and practices in connection with consumer transactions, in violation of Utah Code § 13-11-4 and Utah Code § 13-11-5, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Utah Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately

improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Utah Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and the Utah Protection of Personal Information Act, Utah Code § 13-44-201, which was a direct and proximate cause of the Equifax data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Utah Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Utah Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the

FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*, and the Utah Protection of Personal Information Act, Utah Code § 13-44-201;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Utah Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801, *et seq.*; and the Utah Protection of Personal Information Act, Utah Code § 13-44-201.

1243. Equifax intended to mislead Plaintiff and Utah Subclass members and induce them to rely on its misrepresentations and omissions.

1244. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data

security and ability to protect the confidentiality of consumers' Personal Information.

1245. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Utah Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the Utah Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

1246. Equifax had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extensivity of the Personal Information in its possession, and the generally accepted professional standards in

the credit reporting industry. This duty arose because members of the public, including Plaintiff and the Utah Subclass, repose a trust and confidence in Equifax as one of the nation's entrusted "stewards of data" and Equifax's position as one of three nationwide credit-reporting companies that serve as linchpins of the financial system. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the Utah Subclass, and Equifax because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Equifax. Equifax's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Utah Subclass that contradicted these representations.

1247. Equifax intentionally or knowingly engaged in deceptive acts or practices, violating Utah Code § 13-11-4(2) by:

a. Indicating that the subject of a consumer transaction has sponsorship, approval, performance characteristics, accessories, uses, or benefits, if it has not;

b. Indicating that the subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not;

c. Indicating that the subject of a consumer transaction has been supplied in accordance with a previous representation, if it has not;

d. Indicating that the subject of a consumer transaction will be supplied in greater quantity (e.g. more data security) than the supplier intends.

1248. Equifax engaged in unconscionable acts and practices that were oppressive and led to unfair surprise, as shown in the setting, purpose, and effect of those acts and practices. Equifax's acts and practices unjustly imposed hardship on Plaintiff and the Utah Subclass by imposing on them, through no fault of their own, an increased and imminent risk of fraud and identity theft; substantial cost in time and expenses related to monitoring their financial accounts for fraudulent activity; and lost value of their Personal Information. The deficiencies in Equifax's data security, and the material misrepresentations and omissions concerning those

deficiencies, led to unfair surprise to Plaintiff and the Utah Subclass when the Data Breach occurred.

1249. In addition, there was an overall imbalance in the obligations and rights imposed by the consumer transactions in question, based on the mores and industry standards of the time and place where they occurred. Societal standards required Equifax, as one of the three major credit bureaus, to adequately secure Personal Information in its possession. There is a substantial imbalance between the obligations and rights of consumers, such as Plaintiff and the Utah Subclass, who need access to credit, and Equifax, which has complete control over the Personal Information in its possession. Industry standards—including those reflected in the security requirements of the GLBA—also dictate that Equifax adequately secure the Personal Information in its possession.

1250. Equifax's acts and practices were also procedurally unconscionable because consumers, including Plaintiff and the Utah Subclass, had no practicable option but to have their Personal Information stored in Equifax's systems if they wanted to participate in the nation's financial system. Equifax exploited this imbalance in power, and the asymmetry of information about its data security, to profit by inadequately securing the Personal Information in its systems.

1251. As a direct and proximate result of Equifax's unconscionable and deceptive acts or practices, Plaintiffs and Utah Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1252. Equifax's violations present a continuing risk to Plaintiffs and Utah Subclass members as well as to the general public.

1253. Plaintiff and Utah Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, statutory damages of $2,000 per violation, amounts necessary to avoid unjust enrichment, under Utah Code §§ 13-11-19, *et seq.*; injunctive relief; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE VERMONT SUBCLASS

COUNT 87

VERMONT CONSUMER FRAUD ACT, Vt. Stat. Ann. tit. 9, §§ 2451, *et seq.*

1254. The Vermont Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Vermont Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1255. Plaintiff and Vermont Subclass members are "consumers," as defined by Vt. Stat. Ann. tit. 9, § 2451a(a).

1256. Equifax's conduct as alleged herein related to "goods" or "services" for personal, family, or household purposes, as defined by Vt. Stat. Ann. tit. 9, § 2451a(b).

1257. Equifax is a "seller," as defined by Vt. Stat. Ann. tit. 9, § 2451a(c).

1258. Equifax advertised, offered, or sold goods or services in Vermont and engaged in trade or commerce directly or indirectly affecting the people of Vermont.

1259. Equifax engaged in unfair and deceptive acts or practices, in violation of Vt. Stat. tit. 9, § 2453(a), including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Vermont Subclass

members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Vermont Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and Vermont Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of

Plaintiff and Vermont Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Vermont Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Vermont Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

1260. Equifax intended to mislead Plaintiff and Vermont Subclass members and induce them to rely on its misrepresentations and omissions.

1261. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

1262. Under the circumstances, consumers had a reasonable interpretation of Equifax's representations and omissions.

1263. Equifax had a duty to disclose these facts due to the circumstances of this case, the sensitivity and extensivity of the Personal Information in its possession, and the generally accepted professional standards in the credit reporting industry. This duty arose because members of the public, including Plaintiff and the Vermont Subclass, repose a trust and confidence in Equifax as one of the nation's entrusted "stewards of data" and Equifax's position as one of three nationwide credit-reporting companies that serve as linchpins of the financial system. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiff and the Vermont Subclass, and Equifax because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Equifax. Equifax's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Vermont Subclass that contradicted these representations.

1264. Equifax's acts and practices caused or were likely to cause substantial injury to consumers, which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

1265. The injury to consumers was and is substantial because it was non-trivial and non-speculative; and involved a concrete monetary injury and/or an unwarranted risk to the safety of their Personal Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1266. Consumers could not have reasonably avoided injury because Equifax's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Equifax created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury. Equifax's

business acts and practices also took advantage of its special status as one the nation's three major credit bureaus, making it functionally impossible for consumers to obtain credit without their Personal Information being in Equifax's systems.

1267. Equifax's inadequate data security had no countervailing benefit to consumers or to competition.

1268. Equifax is presumed, as a matter of law under Vt. Stat. Ann. tit. 9, § 2457, to have intentionally violated the Vermont Consumer Protection Act because it failed to sell goods or services in the manner and of the nature advertised or offered.

1269. Equifax acted intentionally, knowingly, and maliciously to violate Vermont's Consumer Fraud Act, and recklessly disregarded Plaintiff and Vermont Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1270. As a direct and proximate result of Equifax's unfair and deceptive acts or practices, Plaintiffs and Vermont Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an

increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1271. Equifax's violations present a continuing risk to Plaintiffs and Vermont Subclass members as well as to the general public.

1272. Plaintiff and Vermont Subclass members seek all monetary and non-monetary relief allowed by law, including injunctive relief, restitution, actual damages, disgorgement of profits, treble damages, punitive/exemplary damages, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE VIRGIN ISLANDS SUBCLASS

COUNT 88

IDENTITY THEFT PREVENTION ACT, V.I. Code tit. 14 §§ 2208, *et seq.*

1273. Plaintiffs, on behalf of the Virgin Islands Subclass, repeat and allege Paragraphs 1-313, as if fully alleged herein.

1274. Equifax is a business that owns or licenses computerized data that includes Personal Information as defined by V.I Code tit. 14 § 2201(a). Equifax also maintains computerized data that includes Personal Information which Equifax does not own. Accordingly, it is subject to V.I Code tit. 14 §§ 2208(a) and (b).

1275. Virgin Islands Subclass members' Personal Information (*e.g.* Social Security numbers) includes Personal Information covered by V.I Code tit. 14 § 2201(a).

1276. Equifax is required to give immediate notice of a breach of security of a data system to owners of Personal Information which Equifax does not own, including Virgin Islands Subclass members, pursuant to V.I Code tit. 14 § 2208(b).

1277. Equifax is required to accurately notify Virgin Islands Subclass members if it discovers a security breach, or receives notice of a security breach which may have compromised Personal Information which Equifax owns or licenses, in the most expedient time possible and without unreasonable delay under V.I Code tit. 14 § 2208(a).

1278. Because Equifax was aware of a security breach, Equifax had an obligation to disclose the data breach as mandated by V.I Code tit. 14 § 2208.

1279. As a direct and proximate result of Equifax's violations of V.I Code tit. 14 §§ 2208(a) and (b), Virgin Islands Subclass members suffered damages, as described above.

1280. Virgin Islands Subclass members seek relief under V.I Code tit. 14 §§ 2211(a) and (b), including actual damages, and injunctive relief.

COUNT 89

VIRGIN ISLANDS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT, V.I. Code tit. 12A, §§ 301, *et seq.*

1281. Plaintiffs, on behalf of the Virgin Islands Subclass, repeat and allege Paragraphs 1-313, as if fully alleged herein.

1282. Equifax is a "person," as defined by V.I. Code tit. 12A, § 303(h).

1283. Plaintiff and Virgin Islands Subclass members are "consumers," as defined by V.I. Code tit. 12A, § 303(d).

1284. Equifax advertised, offered, or sold goods or services in the Virgin Islands and engaged in trade or commerce directly or indirectly affecting the people of the Virgin Islands.

1285. Equifax engaged in unfair and deceptive acts and practices, in violation of V.I. Code tit. 12A, § 304, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Virgin Islands Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately

improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virgin Islands Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and Virgin Islands Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virgin Islands Subclass members' Personal Information, including duties imposed by the FTC Act, 15

U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Virgin Islands Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virgin Islands Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

1286. Equifax's acts and practices were "unfair" under V.I. Code tit. 12A, § 304 because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

1287. The injury to consumers from Equifax's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and/or an unwarranted risk to the safety of their Personal Information or the security of their identity or credit. The injury to consumers was

substantial not only because it inflicted harm on a significant and unprecedented number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1288. Consumers could not have reasonably avoided injury because Equifax's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Equifax created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury. Equifax's business acts and practices also took advantage of its special status as one the nation's three major credit bureaus, making it functionally impossible for consumers to obtain credit without their Personal Information being in Equifax's systems.

1289. Equifax's inadequate data security had no countervailing benefit to consumers or to competition.

1290. Equifax's acts and practices were "deceptive" under V.I. Code tit. 12A, §§ 303 & 304 because Equifax made representations or omissions of material facts that had the capacity, tendency or effect of deceiving or misleading consumers, including Plaintiff and Virgin Islands Subclass members.

1291. Equifax intended to mislead Plaintiff and Virgin Island Subclass members and induce them to rely on its misrepresentations and omissions.

1292. Equifax's representations and omissions were material because they were likely to unfairly influence or deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

1293. Equifax had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the Personal Information in its possession, and the generally accepted professional standards in the credit reporting industry. This duty arose because members of the public, including Plaintiff and the Virgin Islands Subclass, repose a trust and confidence in Equifax as one of the nation's entrusted "stewards of data" and Equifax's position as one of three nationwide credit-reporting companies that serve as linchpins of the financial system. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Virgin Islands Subclass—and Equifax, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Equifax. Equifax's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Virgin Islands Subclass that contradicted these representations.

1294. Equifax acted intentionally, knowingly, and maliciously to violate the Virgin Island's Consumer Fraud and Deceptive Business Practices Act, and recklessly disregarded Plaintiff and Virgin Islands Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate. Equifax intentionally hid the inadequacies in its data security, callously disregarding the rights of consumers.

1295. As a direct and proximate result of Equifax's unfair and deceptive acts or practices, Plaintiff and Virgin Islands Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an

increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1296. Equifax's violations present a continuing risk to Plaintiff and Virgin Islands Subclass members as well as to the general public.

1297. Plaintiff and Virgin Islands Subclass members seek all monetary and non-monetary relief allowed by law, including compensatory, consequential, treble, punitive, and equitable damages under V.I. Code tit. 12A, § 331; injunctive relief; and reasonable attorneys' fees and costs.

COUNT 90

VIRGIN ISLANDS CONSUMER PROTECTION LAW, V.I. Code tit. 12A, §§101, *et seq.*

1298. Plaintiffs, on behalf of the Virgin Islands Subclass, repeat and allege Paragraphs 1-313, as if fully alleged herein.

1299. Equifax is a "merchant," as defined by V.I. Code tit. 12A, § 102(e).

1300. Plaintiff and Virgin Islands Subclass members are "consumers," as defined by V.I. Code tit. 12A, § 102(d).

1301. Equifax sells and offers for sale "consumer goods" and "consumer services," as defined by V.I. Code tit. 12A, § 102(c).

1302. Equifax engaged in deceptive acts and practices, in violation of V.I. Code tit. 12A, § 101, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Virgin Islands Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virgin Islands Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and Virgin Islands Subclass

members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virgin Islands Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Virgin Islands Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virgin Islands Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

1303. Equifax's acts and practices were "deceptive trade practices" under V.I. Code tit. 12A, § 102(a) because Equifax:

a. Represented that goods or services have sponsorship, approval, accessories, characteristics, ingredients, uses, benefits, or quantities that they do not have; or that goods or services are of particular standard, quality, grade, style or model, if they are of another;

b. Used exaggeration, innuendo or ambiguity as to a material fact or failure to state a material fact if such use deceives or tends to deceive;

c. Offered goods or services with intent not to sell them as offered; and

d. Stated that a consumer transaction involves consumer rights, remedies or obligations that it does not involve.

1304. Equifax's acts and practices were also "deceptive" under V.I. Code tit. 12A, § 101 because Equifax made representations or omissions of material facts that had the capacity, tendency or effect of deceiving or misleading consumers, including Plaintiff and Virgin Islands Subclass members.

1305. Equifax intended to mislead Plaintiff and Virgin Islands Subclass members and induce them to rely on its misrepresentations and omissions.

1306. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

1307. Equifax had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the Personal Information in its possession, and the generally accepted professional standards in the credit reporting industry. This duty arose because members of the public, including Plaintiff and the Virgin Islands Subclass, repose a trust and confidence in Equifax as one of the nation's entrusted "stewards of data" and Equifax's position as one of three nationwide credit-reporting companies that serve as linchpins of the financial system. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Virgin Islands Subclass—and Equifax, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Equifax. Equifax's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Virgin Islands Subclass that contradicted these representations.

1308. Equifax acted intentionally, knowingly, and maliciously to violate the Virgin Island's Consumer ProtectionLaw, and recklessly disregarded Plaintiff and Virgin Island Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1309. As a direct and proximate result of Equifax's deceptive acts or practices, Plaintiff and Virgin Islands Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1310. Equifax's violations present a continuing risk to Plaintiff and Virgin Islands Subclass members as well as to the general public.

1311. Plaintiff and Virgin Islands Subclass members seek all monetary and non-monetary relief allowed by law, including declaratory relief; injunctive relief; the greater of actual damages or $500 per violation; compensatory, consequential, treble, and punitive damages; disgorgement; and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE VIRGINIA SUBCLASS

COUNT 91

VIRGINIA PERSONAL INFORMATION BREACH NOTIFICATION ACT, Va. Code. Ann. §§ 18.2-186.6, *et seq.*

1312. The Virginia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Virginia Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1313. Equifax is required to accurately notify Plaintiff and Virginia Subclass members following discovery or notification of a breach of its data security system if unencrypted or unredacted Personal Information was or is reasonably believed to have been accessed and acquired by an unauthorized person who will, or it is reasonably believed who will, engage in identify theft or another fraud, without unreasonable delay under Va. Code Ann. § 18.2-186.6(B).

1314. Equifax is an entity that owns or licenses computerized data that includes Personal Information as defined by Va. Code Ann. § 18.2-186.6(B).

1315. Plaintiff's and Virginia Subclass members' Personal Information includes Personal Information as covered under Va. Code Ann. § 18.2-186.6(A).

1316. Because Equifax discovered a breach of its security system in which unencrypted or unredacted Personal Information was or is reasonably believed to have been accessed and acquired by an unauthorized person, who will, or it is reasonably believed who will, engage in identify theft or another fraud, Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Va. Code Ann. § 18.2-186.6(B).

1317. By failing to disclose the Equifax data breach in a timely and accurate manner, Equifax violated Va. Code Ann. § 18.2-186.6(B).

1318. As a direct and proximate result of Equifax's violations of Va. Code Ann. § 18.2-186.6(B), Plaintiff and Virginia Subclass members suffered damages, as described above.

1319. Plaintiff and Virginia Subclass members seek relief under Va. Code Ann. § 18.2-186.6(I), including actual damages.

COUNT 92

VIRGINIA CONSUMER PROTECTION ACT, Va. Code Ann. §§ 59.1-196, *et seq.*

1320. The Virginia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Virginia Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1321. The Virginia Consumer Protection Act prohibits "[u]sing any . . . deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction." Va. Code Ann. § 59.1-200(14).

1322. Equifax is a "person" as defined by Va. Code Ann. § 59.1-198.

1323. Equifax is a "supplier," as defined by Va. Code Ann. § 59.1-198.

1324. Equifax engaged in the complained-of conduct in connection with "consumer transactions" with regard to "goods" and "services," as defined by Va. Code Ann. § 59.1-198. Equifax advertised, offered, or sold goods or services used primarily for personal, family or household purposes; or relating to an individual's finding or obtaining employment (such as furnishing credit reports to prospective employers).

1325. Equifax engaged in deceptive acts and practices by using deception, fraud, false pretense, false promise, and misrepresentation in connection with consumer transactions, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Virginia Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virginia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and Virginia Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virginia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Virginia Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Virginia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

1326. Equifax intended to mislead Plaintiff and Virginia Subclass members and induce them to rely on its misrepresentations and omissions.

1327. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiff and Virginia

Subclass members, about the adequacy of Equifax's computer and data security and the quality of the Equifax brand.

1328. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the Virginia Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the Virginia Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

1329. In Equifax had a duty to disclose these facts due to the circumstances of this case, the sensitivity and extensivity of the Personal Information in its possession, and the generally accepted professional standards in the credit

reporting industry. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Virginia Subclass—and Equifax, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Equifax. Equifax's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Virginia Subclass that contradicted these representations.

1330. The above-described deceptive acts and practices also violated the following provisions of VA Code § 59.1-200(A):

a. Misrepresenting that goods or services have certain quantities, characteristics, ingredients, uses, or benefits;

b. Misrepresenting that goods or services are of a particular standard, quality, grade, style, or model; and

c. Advertising goods or services with intent not to sell them as advertised, or with intent not to sell them upon the terms advertised.

1331. Equifax acted intentionally, knowingly, and maliciously to violate Virginia's Consumer Protection Act, and recklessly disregarded Plaintiff and Virginia Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate. An award of punitive damages would serve to punish Equifax for its wrongdoing, and warn or deter others from engaging in similar conduct.

1332. As a direct and proximate result of Equifax's deceptive acts or practices, Plaintiffs and Virginia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1333. Equifax's violations present a continuing risk to Plaintiffs and Virginia Subclass members as well as to the general public.

1334. Plaintiff and Virginia Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages; statutory damages in the amount of $1,000 per violation if the conduct is found to be willful or, in the alternative, $500 per violation; restitution, injunctive relief; punitive damages; and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE WASHINGTON SUBCLASS

COUNT 93

WASHINGTON DATA BREACH NOTICE ACT, Wash. Rev. Code §§ 19.255.010, *et seq.*

1335. The Washington Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Washington Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1336. Equifax is a business that owns or licenses computerized data that includes Personal Information as defined by Wash. Rev. Code § 19.255.010(1).

1337. Plaintiff's and Washington Subclass members' Personal Information includes Personal Information as covered under Wash. Rev. Code § 19.255.010(5).

1338. Equifax is required to accurately notify Plaintiff and Washington Subclass members following discovery or notification of the breach of its data security system if Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Personal Information was not

secured, in the most expedient time possible and without unreasonable delay under Wash. Rev. Code § 19.255.010(1).

1339. Because Equifax discovered a breach of its security system in which Personal Information was, or is reasonably believed to have been, acquired by an unauthorized person and the Personal Information was not secured, Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wash. Rev. Code § 19.255.010(1).

1340. By failing to disclose the Equifax data breach in a timely and accurate manner, Equifax violated Wash. Rev. Code § 19.255.010(1).

1341. As a direct and proximate result of Equifax's violations of Wash. Rev. Code § 19.255.010(1), Plaintiff and Washington Subclass members suffered damages, as described above.

1342. Plaintiff and Washington Subclass members seek relief under Wash. Rev. Code §§ 19.255.010(13)(a) and 19.255.010(13)(b), including actual damages and injunctive relief.

COUNT 94

WASHINGTON CONSUMER PROTECTION ACT, Wash. Rev. Code Ann. §§ 19.86.020, *et seq.*

1343. The Washington Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Washington Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1344. Equifax is a "person," as defined by Wash. Rev. Code Ann. § 19.86.010(1).

1345. Equifax advertised, offered, or sold goods or services in Washington and engaged in trade or commerce directly or indirectly affecting the people of Washington, as defined by Wash. Rev. Code Ann. § 19.86.010 (2).

1346. Equifax engaged in unfair or deceptive acts or practices in the conduct of trade or commerce, in violation of Wash. Rev. Code Ann. § 19.86.020, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Washington Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately

improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Washington Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and Washington Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Washington Subclass members' Personal Information, including duties imposed by the FTC Act, 15

U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Washington Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Washington Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

1347. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

1348. Equifax acted intentionally, knowingly, and maliciously to violate Washington's Consumer Protection Act, and recklessly disregarded Plaintiff and

Washington Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1349. Equifax's conduct is injurious to the public interest because it violates Wash. Rev. Code Ann. § 19.86.020, violates a statute that contains a specific legislation declaration of public interest impact, and/or injured persons and had and has the capacity to injure persons. Further, its conduct affected the public interest, including the millions of Washingtonians affected by the Equifax Data Breach.

1350. As a direct and proximate result of Equifax's unfair methods of competition and unfair or deceptive acts or practices, Plaintiff and Washington Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1351. Plaintiff and Washington Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, injunctive relief, civil penalties, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE WEST VIRGINIA SUBCLASS

COUNT 95

WEST VIRGINIA CONSUMER CREDIT AND PROTECTION ACT, W. Va. Code §§ 46A-6-101, *et seq.*

1352. The West Virginia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the West Virginia Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1353. Plaintiff and West Virginia Subclass members are "consumers," as defined by W. Va. Code § 46A-6-102(2).

1354. Equifax engaged in "consumer transactions," as defined by W. Va. Code § 46A-6-102(2).

1355. Equifax advertised, offered, or sold goods or services in West Virginia and engaged in trade or commerce directly or indirectly affecting the people of West Virginia, as defined by W. Va. Code § 46A-6-102(6).

1356. Plaintiff sent a demand for relief on behalf of the West Virginia Subclass pursuant to W. Va. Code § 46A-6-106(c) on October 10, 2017. Equifax has not cured its unfair and deceptive acts and practices.

1357. Equifax engaged in unfair and deceptive business acts and practices in the conduct of trade or commerce, in violation of W. Va. Code § 46A-6-104, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and West Virginia Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and West Virginia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and West Virginia Subclass

members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and West Virginia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and West Virginia Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and West Virginia Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

1358. Equifax's unfair and deceptive acts and practices also violated W. Va. Code § 46A-6-102(7), including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;

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

c. Advertising goods or services with intent not to sell them as advertised;

d. Engaging in any other conduct which similarly creates a likelihood of confusion or of misunderstanding;

e. Using deception, fraud, false pretense, false promise or misrepresentation, or the concealment, suppression or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of goods or services, whether or not any person has in fact been misled, deceived or damaged thereby; and

f. Advertising, displaying, publishing, distributing, or causing to be advertised, displayed, published, or distributed in any manner, statements and representations with regard to the sale of goods or the extension of consumer credit, which are false, misleading or deceptive or which omit to state material information which is necessary to make the statements therein not false, misleading or deceptive.

1359. Equifax's unfair and deceptive acts and practices were unreasonable when weighed against the need to develop or preserve business, and were injurious to the public interest, under W. Va. Code § 46A-6-101.

1360. Equifax's acts and practices were additionally "unfair" under W. Va. Code § 46A-6-104 because they caused or were likely to cause substantial injury to consumers which was not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.

1361. The injury to consumers from Equifax's conduct was and is substantial because it was non-trivial and non-speculative; and involved a monetary injury and/or an unwarranted risk to the safety of their Personal Information or the security of their identity or credit. The injury to consumers was substantial not only because it inflicted harm on a significant and unprecedented

number of consumers, but also because it inflicted a significant amount of harm on each consumer.

1362. Consumers could not have reasonably avoided injury because Equifax's business acts and practices unreasonably created or took advantage of an obstacle to the free exercise of consumer decision-making. By withholding important information from consumers about the inadequacy of its data security, Equifax created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury. Equifax's business acts and practices made it functionally impossible for consumers to obtain credit without their Personal Information being in Equifax's systems.

1363. Equifax's inadequate data security had no countervailing benefit to consumers or to competition.

1364. Equifax's acts and practices were additionally "deceptive" under W. Va. Code § 46A-6-104 because Equifax made representations or omissions of material facts that misled or were likely to mislead reasonable consumers, including Plaintiff and West Virginia Subclass members.

1365. Equifax intended to mislead Plaintiff and West Virginia Subclass members and induce them to rely on its misrepresentations and omissions.

1366. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

1367. 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 serve as trusted linchpins of the financial system, and Equifax was trusted with sensitive and valuable Personal Information regarding hundreds of millions of consumers, including Plaintiff and the West Virginia Subclass. Equifax accepted the responsibility of being a "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, Plaintiff and the West Virginia Subclass members acted reasonably in relying on Equifax's misrepresentations and omissions, the truth of which they could not have discovered.

1368. Equifax had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the Personal Information in its possession, and the generally accepted professional standards in the credit reporting industry. This duty arose because members of the public, including Plaintiff and the West Virginia Subclass, repose a trust and confidence in Equifax as one of the nation's entrusted "stewards of data" and Equifax's position as one of three nationwide credit-reporting companies that serve as linchpins of the financial system. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the West Virginia Subclass—and Equifax, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Equifax. Equifax's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and

the West Virginia Subclass that contradicted these representations.

1369. Equifax's omissions were legally presumed to be equivalent to active misrepresentations because Equifax intentionally prevented Plaintiff and West Virginia Subclass members from discovering the truth regarding Equifax's inadequate data security.

1370. Equifax acted intentionally, knowingly, and maliciously to violate West Virginia's Consumer Credit and Protection Act, and recklessly disregarded Plaintiff and West Virginia Subclass members' rights. Equifax's unfair and deceptive acts and practices were likely to cause serious harm. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1371. As a direct and proximate result of Equifax's unfair and deceptive acts or practices and Plaintiff and West Virginia Subclass members' purchase of goods or services, Plaintiff and West Virginia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity;

an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

1372. Equifax's violations present a continuing risk to Plaintiff and West Virginia Subclass members as well as to the general public.

1373. Plaintiff and West Virginia Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $200 per violation under W. Va. Code § 46A-6-106(a); restitution, injunctive and other equitable relief; punitive damages, and reasonable attorneys' fees and costs.

CLAIMS ON BEHALF OF THE WISCONSIN SUBCLASS

COUNT 96

NOTICE OF UNAUTHORIZED ACQUISITION OF PERSONAL INFORMATION, Wis. Stat. §§ 134.98(2), *et seq.*

1374. The Wisconsin Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Wisconsin Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1375. Equifax is a business that maintains or licenses Personal Information as defined by Wis. Stat. § 134.98(2).

1376. Plaintiff's and Wisconsin Subclass members' Personal Information (*e.g.*, Social Security numbers) includes Personal Information as covered under Wis. Stat. § 134.98(1)(b).

1377. Equifax is required to accurately notify Plaintiff and Wisconsin Subclass members if it knows that Personal Information in its possession has been acquired by a person whom it has not authorized to acquire the Personal Information within a reasonable time under Wis. Stat. §§ 134.98(2)-(3)(a).

1378. Because Equifax knew that Personal Information in its possession had been acquired by a person whom it has not authorized to acquire the Personal Information, Equifax had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Wis. Stat. § 134.98(2).

1379. By failing to disclose the Equifax data breach in a timely and accurate manner, Equifax violated Wis. Stat. § 134.98(2).

1380. As a direct and proximate result of Equifax's violations of Wis. Stat. § 134.98(3)(a), Plaintiff and Wisconsin Subclass members suffered damages, as described above.

1381. Plaintiff and Wisconsin Subclass members seek relief under Wis. Stat. § 134.98, including actual damages and injunctive relief.

COUNT 97

WISCONSIN DECEPTIVE TRADE PRACTICES ACT, Wis. Stat. § 100.18

1382. The Wisconsin Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Wisconsin Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1383. Equifax is a "person, firm, corporation or association," as defined by Wis. Stat. § 100.18(1).

1384. Plaintiff and Wisconsin Subclass members are members of "the public," as defined by Wis. Stat. § 100.18(1).

1385. With intent to sell, distribute, or increase consumption of merchandise, services, or anything else offered by Equifax to members of the public for sale, use, or distribution, Equifax made, published, circulated, placed before the public or caused (directly or indirectly) to be made, published, circulated, or placed before the public in Wisconsin advertisements, announcements, statements, and representations to the public which contained assertions, representations, or statements of fact which are untrue, deceptive, and/or misleading, in violation of Wis. Stat. § 100.18(1).

1386. Equifax also engaged in the above-described conduct as part of a plan or scheme, the purpose or effect of which was to sell, purchase, or use merchandise or services not as advertised, in violation of Wis. Stat. § 100.18(9).

1387. Equifax's deceptive acts, practices, plans, and schemes include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Wisconsin Subclass members' Personal Information, which was a direct and proximate cause of the Equifax data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Equifax data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Wisconsin Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, 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 the privacy and confidentiality of Plaintiff and Wisconsin Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Wisconsin Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Wisconsin Subclass members' Personal Information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Wisconsin Subclass members' Personal Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

1388. Equifax intended to mislead Plaintiff and Wisconsin Subclass members and induce them to rely on its misrepresentations and omissions.

1389. Equifax's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Equifax's data security and ability to protect the confidentiality of consumers' Personal Information.

1390. Equifax had a duty to disclose the above-described facts due to the circumstances of this case, the sensitivity and extensivity of the Personal Information in its possession, and the generally accepted professional standards in the credit reporting industry. This duty arose because members of the public, including Plaintiff and the Wisconsin Subclass, repose a trust and confidence in Equifax as one of the nation's entrusted "stewards of data" and Equifax's position as one of three nationwide credit-reporting companies that serve as linchpins of the financial system. In addition, such a duty is implied by law due to the nature of the relationship between consumers—including Plaintiff and the Wisconsin Subclass—and Equifax, because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in Equifax. Equifax's duty to disclose also arose from its:

a. Possession of exclusive knowledge regarding the security of the data in its systems;

b. Active concealment of the state of its security; and/or

c. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiff and the Wisconsin Subclass that contradicted these representations.

1391. Equifax's failure to disclose the above-described facts is the same as actively representing that those facts do not exist.

1392. Equifax acted intentionally, knowingly, and maliciously to violate the Wisconsin Deceptive Trade Practices Act, and recklessly disregarded Plaintiff and Wisconsin Subclass members' rights. Equifax's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

1393. As a direct and proximate result of Equifax's deceptive acts or practices, Plaintiff and Wisconsin Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an

increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information..

1394. Equifax had an ongoing duty to all Equifax customers to refrain from deceptive acts, practices, plans, and schemes under Wis. Stat. § 100.18.

1395. Plaintiff and Wisconsin Subclass members seek all monetary and non-monetary relief allowed by law, including damages, reasonable attorneys' fees, and costs under Wis. Stat. § 100.18(11)(b)(2), injunctive relief, and punitive damages.

CLAIMS ON BEHALF OF THE WYOMING SUBCLASS

COUNT 98

COMPUTER SECURITY BREACH; NOTICE TO AFFECTED PERSONS, Wyo. Stat. Ann. §§ 40-12-502(a), *et seq.*

1396. The Wyoming Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Wyoming Subclass, repeats and alleges Paragraphs 1-313, as if fully alleged herein.

1397. Equifax is a business that owns or licenses computerized data that includes Personal Information as defined by Wyo. Stat. Ann. § 40-12-502(a).

1398. Plaintiff's and Wyoming Subclass members' Personal Information (*e.g.*, Social Security numbers) includes Personal Information as covered under Wyo. Stat. Ann. § 40-12-502(a).

1399. Equifax is required to accurately notify Plaintiff and Wyoming Subclass members when it becomes aware of a breach of its data security system if the misuse of personal identifying information has occurred or is reasonably likely to occur, in the most expedient time possible and without unreasonable delay under Wyo. Stat. Ann. § 40-12-502(a).

1400. Because Equifax was aware of a breach of its data security system in which the misuse of personal identifying information has occurred or is reasonably likely to occur, Equifax had an obligation to disclose the Equifax data breach in a timely and accurate fashion as mandated by Wyo. Stat. Ann. § 40-12-502(a).

1401. By failing to disclose the Equifax data breach in a timely and accurate manner, Equifax violated Wyo. Stat. Ann. § 40-12-502(a).

1402. As a direct and proximate result of Equifax's violations of Wyo. Stat. Ann. § 40-12-502(a), Plaintiff and Wyoming Subclass members suffered damages, as described above.

1403. Plaintiff and Equifax Subclass members seek relief under Wyo. Stat. Ann. § 40-12-502(f), including actual damages and equitable relief.

RECOVERY OF EXPENSES OF LITIGATION ON BEHALF OF ALL PLAINTIFFS

COUNT 99

O.C.G.A. § 13-6-11

1404. Pursuant to O.C.G.A. § 13-6-11, the jury may allow the expenses of litigation and attorneys' fees as part of the damages where a defendant "has acted in bad faith, has been stubbornly litigious, or has caused the plaintiff unnecessary trouble and expense."

1405. 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.

1406. 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.

REQUEST FOR RELIEF

Plaintiffs, individually and on behalf of members of the Class and Subclasses, as applicable, respectfully request that the Court enter judgment in their favor and against Equifax, as follows:

1. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiffs are proper class representatives; and appoint Plaintiffs' Co-Lead and Co-Liaison Counsel as Class Counsel;

2. That the Court grant permanent injunctive relief to prohibit Equifax from continuing to engage in the unlawful acts, omissions, and practices described herein;

3. That the Court award Plaintiffs and Class and Subclass members compensatory, consequential, general, and nominal damages in an amount to be determined at trial;

4. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Equifax as a result of its unlawful acts, omissions, and practices;

5. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

6. That Plaintiffs be granted the declaratory relief sought herein;

7. That the Court award to Plaintiffs the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

8. That the Court allow as part of damages and award to Plaintiffs their expenses of litigation and attorneys' fees pursuant to O.C.G.A. § 13-6-11;

9. That the Court award pre- and post-judgment interest at the maximum legal rate; and

10. That the Court grant all such other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial on all claims so triable.

Dated: May 14, 2018

Respectfully submitted,

/s/ Amy E. Keller
Amy E. Keller
Adam J. Levitt
DiCELLO LEVITT & CASEY LLC
Ten North Dearborn Street
Eleventh Floor
Chicago, Illinois 60602
Tel. 312.214.7900
akeller@dlcfirm.com
alevitt@dlcfirm.com

/s/ Kenneth S. Canfield
Kenneth S. Canfield
Georgia Bar No. 107744
DOFFERMYRE SHIELDS CANFIELD & KNOWLES, LLC
1355 Peachtree Street, N.E.
Suite 1900
Atlanta, Georgia 30309
Tel. 404.881.8900
kcanfield@dsckd.com

/s/ Norman E. Siegel
Norman E. Siegel
Barrett J. Vahle
J. Austin Moore
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Tel. 816.714.7100
siegel@stuevesiegel.com
vahle@stuevesiegel.com
moore@stuevesiegel.com

Consumer Plaintiffs' Co-Lead Counsel

Roy E. Barnes
John R. Bevis
J. Cameron Tribble
BARNES LAW GROUP, LLC
31 Atlanta Street
Marietta, Georgia 30060
Tel. 770.227.6375
roy@barneslawgroup.com
bevis@barneslawgroup.com
ctribble@barneslawgroup.com

David J. Worley
EVANGELISTA WORLEY LLC
8100A Roswell Road Suite 100
Atlanta, Georgia 30350
Tel. 404.205.8400
david@ewlawllc.com

Consumer Plaintiffs' Co-Liaison Counsel

Rodney K. Strong
GRIFFIN & STRONG P.C.
235 Peachtree Street NE, Suite 400
Atlanta, Georgia 30303
Tel. 404.584.9777
rodney@gspclaw.com
Consumer Plaintiffs' State Court Coordinating Counsel

Andrew N. Friedman
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Avenue, NW
Suite 500
Washington, D.C. 20005
Tel. 202.408.4600
afriedman@cohenmilstein.com

Eric H. Gibbs
David M. Berger
GIRARD GIBBS LLP
505 14th Street
Suite 1110
Oakland, California 94612
Tel. 510.350.9700
ehg@classlawgroup.com

James Pizzirusso
HAUSFELD LLP
1700 K Street NW Suite 650
Washington, D.C. 20006
Tel. 202.540.7200
jpizzirusso@hausfeld.com

Ariana J. Tadler
MILBERG TADLER PHILLIPS GROSSMAN LLP
One Penn Plaza
19th Floor
New York, New York 10119
Tel. 212.594.5300
atadler@milberg.com

John A. Yanchunis
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Tel. 813.223.5505
jyanchunis@forthepeople.com

William H. Murphy III
MURPHY, FALCON & MURPHY
1 South Street, 23rd Floor
Baltimore, Maryland 21224
Tel. 410.539.6500
hassan.murphy@murphyfalcon.com

Jason R. Doss
THE DOSS FIRM, LLC
36 Trammell Street, Suite 101
Marietta, Georgia 30064
Tel. 770.578.1314
jasondoss@dossfirm.com
Consumer Plaintiffs' Steering Committee

CERTIFICATE OF SERVICE

I hereby certify that a copy of the foregoing was filed with this Court via its CM/ECF service, which will send notification of such filing to all counsel of record this 14th day of May, 2018.

/s/ Norman E. Siegel