

1 Tina Wolfson, CA Bar No. 174806
2 *twolfson@ahdootwolfson.com*
3 **AHDOOT & WOLFSON, PC**
4 1016 Palm Avenue
5 West Hollywood, CA 90069
6 Telephone: (310) 474-9111
7 Fax: (310) 474-8585

8 Daniel S. Robinson, CA Bar No. 244245
9 *drobinson@rcrsd.com*
10 **ROBINSON CALCAGNIE ROBINSON**
11 **SHAPIRO DAVIS, INC.**
12 19 Corporate Plaza Dr.
13 Newport Beach, CA 92660
14 Telephone: (949) 720-1288
15 Fax: (949) 720-1292

16 *Co-Lead Counsel for Plaintiffs and the Proposed Class*
17 *Additional Counsel Listed on Signature Block*

18
19
20
21
22
23
24
25
26
27
28
UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
SOUTHERN DIVISION

**IN RE EXPERIAN DATA BREACH
LITIGATION**

No. SACV 15-1592 AG (DFMx)

**CONSOLIDATED CLASS ACTION
COMPLAINT**

JURY TRIAL DEMANDED

TABLE OF CONTENTS

NATURE OF THE CASE.....	1
PARTIES.....	3
A. Plaintiffs.....	3
B. Defendants.....	27
JURISDICTION AND VENUE.....	27
FACTS.....	28
A. The Data Breach Compromised the PII of 15 Million Consumers.....	28
B. Experian Promised to Protect Its Customers’ PII, but Maintained Inadequate Data Security	32
C. Experian Experienced Prior Data Breaches, but Nevertheless Failed to Implement Appropriate Security	35
D. The Data Breach Has Exposed Plaintiffs and Other Consumers to Fraud, Identity Theft, Financial Harm, and a Heightened, Imminent Risk of Such Harm in the Future	38
E. Experian Was Required to Insure the Security of Plaintiffs’ PII, and to Investigate and Provide Timely and Adequate Notification of the Data Breach under Federal Regulations, But Failed To Do So	42
CLASS ACTION ALLEGATIONS.....	46
A. Nationwide Class	46
B. Statewide Subclasses.....	46
CAUSES OF ACTION.....	51
COUNT 1: WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT	51
COUNT 2: NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT	54
COUNT 3: NEGLIGENCE	54
COUNT 4: NEGLIGENCE PER SE	56

i.	Alabama	59
	COUNT 5: VIOLATION OF THE ALABAMA DECEPTIVE TRADE	
	PRACTICES ACT, Ala. Code § 8-19-1, <i>et seq.</i>	59
ii.	Arizona	62
	COUNT 6: VIOLATION OF THE ARIZONA CONSUMER FRAUD	
	ACT, Ariz. Rev. Stat. § 44-1521, <i>et seq.</i>	62
iii.	California	64
	COUNT 7: VIOLATION OF THE CALIFORNIA UNFAIR	
	COMPETITION LAW, Cal. Bus. & Prof. Code § 17200, <i>et</i>	
	<i>seq.</i>	64
	COUNT 8: VIOLATION OF THE CALIFORNIA CUSTOMER	
	RECORDS ACT, Cal. Civ. Code § 1798.80, <i>et seq.</i>	66
	COUNT 9: VIOLATION OF THE CALIFORNIA CONSUMERS LEGAL	
	REMEDIES ACT, Cal. Civ. Code § 1750, <i>et seq.</i>	68
iv.	Colorado	70
	COUNT 10: VIOLATION OF THE COLORADO CONSUMER	
	PROTECTION ACT, Colo. Rev. Stat. § 6-1-1010, <i>et seq.</i>	70
	COUNT 11: VIOLATION OF THE COLORADO SECURITY BREACH	
	NOTIFICATION ACT, Colo. Rev. Stat. § 6-1-716, <i>et seq.</i>	73
v.	Delaware	74
	COUNT 12: VIOLATION OF THE DELAWARE CONSUMER FRAUD	
	ACT, 6 Del. Code § 2513, <i>et seq.</i>	74
	COUNT 13: VIOLATION OF THE DELAWARE COMPUTER	
	SECURITY BREACH ACT, 6 Del. Code § 12B-102, <i>et</i>	
	<i>seq.</i>	76
vi.	District of Columbia	78

1	COUNT 14: VIOLATION OF THE DISTRICT OF COLUMBIA	
2	CONSUMER PROTECTION PROCEDURES ACT, D.C. Code	
3	§ 28-3904, <i>et seq.</i>	78
4	COUNT 15: VIOLATION OF THE DISTRICT OF COLUMBIA	
5	CONSUMER SECURITY BREACH NOTIFICATION ACT,	
6	D.C. Code § 28-3851, <i>et seq.</i>	80
7	vii. Florida	81
8	COUNT 16: VIOLATION OF THE FLORIDA UNFAIR AND	
9	DECEPTIVE TRADE PRACTICES ACT, Fla. Stat. § 501.201,	
10	<i>et seq.</i>	81
11	viii. Georgia	83
12	COUNT 17: VIOLATION OF THE GEORGIA FAIR BUSINESS	
13	PRACTICES ACT, Ga. Code Ann. § 10-1-390, <i>et seq.</i>	83
14	COUNT 18: VIOLATION OF THE GEORGIA SECURITY BREACH	
15	NOTIFICATION ACT, Ga. Code Ann. § 10-1-912, <i>et seq.</i>	85
16	ix. Hawaii	86
17	COUNT 19: VIOLATION OF THE HAWAII UNFAIR PRACTICES AND	
18	UNFAIR COMPETITION STATUTE, Haw. Rev. Stat. § 480-1,	
19	<i>et seq.</i>	86
20	COUNT 20: VIOLATION OF THE HAWAII SECURITY BREACH	
21	NOTIFICATION ACT, Haw. Rev. Stat. § 487N-1, <i>et seq.</i>	88
22	x. Illinois	90
23	COUNT 21: VIOLATION OF THE ILLINOIS CONSUMER FRAUD ACT,	
24	815 Ill. Comp. Stat. 505/1, <i>et seq.</i>	90
25	COUNT 22: VIOLATION OF THE ILLINOIS UNIFORM DECEPTIVE	
26	TRADE PRACTICES ACT, 815 Ill. Comp. Stat. 510/2, <i>et</i>	
27	<i>seq.</i>	92
28	xi. Indiana	93

1	COUNT 23: VIOLATION OF THE INDIANA DECEPTIVE CONSUMER	
2	SALES ACT, Ind. Code § 24-5-0.5-3, <i>et seq.</i>	93
3	xii. Kentucky	96
4	COUNT 24: VIOLATION OF THE KENTUCKY COMPUTER SECURITY	
5	BREACH NOTIFICATION ACT, Ky. Rev. Stat. Ann. §	
6	365.732, <i>et seq.</i>	96
7	xiii. Massachusetts.....	97
8	COUNT 25: VIOLATION OF THE MASSACHUSETTS CONSUMER	
9	PROTECTION ACT, Mass. Gen. Laws Ann. ch. 93A, § 1, <i>et</i>	
10	<i>seq.</i>	97
11	xiv. Michigan	99
12	COUNT 26: VIOLATION OF THE MICHIGAN CONSUMER	
13	PROTECTION ACT, Mich. Comp. Laws § 445.903, <i>et seq.</i>	99
14	COUNT 27: VIOLATION OF THE MICHIGAN IDENTITY THEFT	
15	PROTECTION ACT, Mich. Comp. Laws § 445.72, <i>et seq.</i>	101
16	xv. Minnesota.....	103
17	COUNT 28: VIOLATION OF THE MINNESOTA PREVENTION OF	
18	CONSUMER FRAUD ACT, Minn. Stat. §§ 325F.68 & 8.31, <i>et</i>	
19	<i>seq.</i>	103
20	COUNT 29: VIOLATION OF THE MINNESOTA UNIFORM	
21	DECEPTIVE TRADE PRACTICES ACT, Minn. Stat. §	
22	325D.43, <i>et seq.</i>	105
23	xvi. Missouri	107
24	COUNT 30: VIOLATION OF THE MISSOURI MERCHANDISE	
25	PRACTICING ACT, Mo. Stat. § 407.010, <i>et seq.</i>	107
26	xvii. Nevada	109

1	COUNT 31: VIOLATION OF THE NEVADA DECEPTIVE TRADE	
2	PRACTICES ACT, Nev. Rev. Stat. Ann. § 598.0915, <i>et</i>	
3	<i>seq.</i>	109
4	xviii. New Jersey	111
5	COUNT 32: VIOLATION OF THE NEW JERSEY CONSUMER FRAUD	
6	ACT, N.J. Stat. Ann. § 56:8-1, <i>et seq.</i>	111
7	COUNT 33: VIOLATION OF THE NEW JERSEY CUSTOMER	
8	SECURITY BREACH DISCLOSURE ACT, N.J. Stat. Ann. §	
9	56:8-163, <i>et seq.</i>	113
10	xix. New Mexico	114
11	COUNT 34: VIOLATION OF THE NEW MEXICO UNFAIR PRACTICES	
12	ACT, N.M. Stat. Ann. § 57-12-2, <i>et seq.</i>	114
13	xx. New York	116
14	COUNT 35: VIOLATION OF THE NEW YORK GENERAL BUSINESS	
15	LAW, N.Y. Gen. Bus. Law § 349, <i>et seq.</i>	116
16	xxi. North Carolina	118
17	COUNT 36: VIOLATION OF THE NORTH CAROLINA UNFAIR	
18	TRADE PRACTICES ACT, N.C. Gen. Stat. Ann. § 75-1.1, <i>et</i>	
19	<i>seq.</i>	118
20	xxii. Ohio	120
21	COUNT 37: VIOLATION OF THE OHIO CONSUMER SALES	
22	PRACTICES ACT, Ohio Rev. Code § 1345.01, <i>et seq.</i>	120
23	COUNT 38: VIOLATION OF THE OHIO DECEPTIVE TRADE	
24	PRACTICES ACT, Ohio Rev. Code § 4165.01, <i>et seq.</i>	122
25	xxiii. Oregon	124
26	COUNT 39: VIOLATION OF THE OREGON UNLAWFUL TRADE	
27	PRACTICES ACT, Or. Rev. Stat. § 646.608, <i>et seq.</i>	124
28		

1	COUNT 40: VIOLATION OF THE OREGON CONSUMER IDENTITY	
2	THEFT PROTECTION ACT, Or. Rev. Stat. § 646A.600, <i>et</i>	
3	<i>seq.</i>	126
4	xxiv. Pennsylvania	128
5	COUNT 41: VIOLATION OF THE PENNSYLVANIA UNFAIR TRADE	
6	PRACTICES AND CONSUMER PROTECTION ACT, 73 Pa.	
7	Stat. §§ 201-2 & 201-3, <i>et seq.</i>	128
8	xxv. South Carolina.....	130
9	COUNT 42: VIOLATION OF THE SOUTH CAROLINA DATA BREACH	
10	SECURITY ACT, S.C. Code Ann. § 39-1-90, <i>et seq.</i>	130
11	xxvi. Tennessee	131
12	COUNT 43: VIOLATION OF THE TENNESSEE PERSONAL	
13	CONSUMER INFORMATION RELEASE ACT, Tenn. Code	
14	Ann. § 47-18-2107, <i>et seq.</i>	131
15	xxvii. Texas	132
16	COUNT 44: VIOLATION OF THE TEXAS DECEPTIVE TRADE	
17	PRACTICES-CONSUMER PROTECTION ACT, Tex. Bus. &	
18	Com. Code § 17.46, <i>et seq.</i>	132
19	xxviii. Virginia	135
20	COUNT 45: VIOLATION OF THE VIRGINIA CONSUMER	
21	PROTECTION ACT, Va. Code Ann. § 59.1-196, <i>et seq.</i>	135
22	COUNT 46: VIOLATION OF THE VIRGINIA PERSONAL	
23	INFORMATION BREACH NOTIFICATION ACT, Va. Code	
24	Ann. § 18.2-186.6, <i>et seq.</i>	137
25	xxix. Washington	138
26	COUNT 47: VIOLATION OF THE WASHINGTON CONSUMER	
27	PROTECTION ACT, Wash. Rev. Code Ann. § 19.86.020, <i>et</i>	
28	<i>seq.</i>	138

1 COUNT 48: VIOLATION OF THE WASHINGTON DATA BREACH

2 NOTICE ACT, Wash. Rev. Code Ann. § 19.255.010, *et*

3 *seq.* 140

4 RELIEF REQUESTED 142

5 DEMAND FOR JURY TRIAL 143

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

1 Plaintiffs,¹ individually and on behalf of the classes defined below, bring this
 2 Consolidated Class Action Complaint (“Complaint”) against Experian Information
 3 Solutions, Inc. and Experian Holdings, Inc. (collectively, “Experian” or “Defendants”),
 4 and allege as follows:

5 NATURE OF THE CASE

6 1. On October 1, 2015, Experian announced a nationwide data breach
 7 affecting an estimated 15 million consumers (the “Data Breach”). According to
 8 Experian’s press release, unauthorized parties accessed consumers’ sensitive, personal
 9 information maintained on Experian’s servers, including the information of T-Mobile
 10 users. The information included names, addresses, Social Security numbers, dates of
 11 birth, driver’s license numbers, military ID numbers, passport numbers, and other
 12 personally identifiable information (collectively, “PII”) used in T-Mobile’s credit
 13 assessment.² On October 8, 2015, Experian announced that the information accessed in
 14 the Data Breach included the personal information of unidentified organizations and
 15 individuals in addition to T-Mobile customers.³

16 2. The Data Breach occurred because Experian failed to implement adequate
 17 security measures to safeguard consumers’ PII and willfully ignored *known*
 18 weaknesses in its data security, including prior hacks into its information systems.
 19 Unauthorized parties routinely attempt to gain access to and steal personal information
 20 from networks and information systems—especially from entities such as Experian,

21
 22 ¹ “Plaintiffs” refers collectively to Plaintiffs Stephen Allen, Richard Parks, Ryan Hamre,
 23 Joshua Gonzales, Gwendolyn Crump, Elleen Brazzle, Melissa Merry, Francisco Ojeda,
 24 Alison Cochran, Alice Dunscomb, Jessica Holt, Samantha Manganaris, Veronica
 25 Gillotte, David Brown, Stuart Zimmelman, Chris Shearer, Christiaan Mealey, Gregory
 26 Hertik, Allan Sommercorn, Kamil Kuklinski, Charles Yoo, Sergey Barbashov, Kathleen
 27 Alcorn, Mary Roberts, Tony George, Ryan Heitz, Gerardus Jansen, Lorenzo Jackson,
 28 Eban Liebig, Angelia Fennern, Charles Sallade, Cregan Smith, Giovanni Williams,
 Dipak Bhuta, Joseph Zubrzycki, Lucio Hernandez, Shivan Bassaw, Jennifer Looney,
 Darius Clark, Hunter Graham, Philip Popiel, John Reiser, Jennifer Brandabur, Perry
 Heath, David Lumb, Martha Cebrian-Vega, Mark Hodson, Daisy Hodson, Amjed
 Ababseh, Martha Schroeder, Jason Shafer, Nathaniel Apan, and Jeffrey Gutschmidt.

² See *Overview: Unauthorized Acquisition of Personal Information*, EXPERIAN,
<http://www.experian.com/data-breach/t-mobilefacts.html> (last visited Oct. 15, 2015).

³ See *id.*

1 which are known to possess a large number of individuals' valuable personal and
2 financial information.

3 3. Armed with the personal information obtained in the Data Breach, identity
4 thieves can commit a variety of crimes that harm victims of the Data Breach. For
5 instance, they can take out loans, mortgage property, and open financial accounts and
6 open credit cards in a victim's name; use a victim's information to obtain government
7 benefits or file fraudulent returns to obtain a tax refund; obtain a driver's license or
8 identification card in a victim's name; gain employment in a victim's name; obtain
9 medical services in a victim's name; or give false information to police during an arrest.
10 Hackers also routinely sell individuals' PII to other criminals who intend to misuse the
11 information. According to third party security experts, the PII obtained from the Data
12 Breach was available for sale on the dark web, precisely for such nefarious purposes.

13 4. As a result of Experian's willful failure to prevent the breach, Plaintiffs and
14 Class members have been exposed to fraud, identity theft, and financial harm, as
15 detailed below, and to a heightened, imminent risk of such harm in the future. Plaintiffs
16 and Class members have to monitor their financial accounts and credit histories more
17 closely and frequently to guard against identity theft. Class members also have
18 incurred, and will continue to incur, additional out-of-pocket costs for obtaining credit
19 reports, credit freezes, credit monitoring services, and other protective measures in order
20 to detect, protect, and repair the Data Breach's impact on their PII for the remainder of
21 their lives. Plaintiffs anticipate spending considerable time and money for the rest of
22 their lives in order to detect and respond to the impact of the Data Breach.

23 5. Many class members have already suffered fraud as a result of the Data
24 Breach. Others may have been but don't know it yet. There is a strong likelihood that
25 these and other Class members will become victims of identity fraud in the future given
26 the breadth of their PII that is now publicly available. Javelin Strategy & Research
27 reported in its 2014 Identity Fraud Study that "[d]ata breaches are the greatest risk
28 factor for identity fraud." In fact, "[i]n 2013, one in three consumers who received

1 notification of a data breach became a victim of fraud.” Javelin also found increased
2 instances of fraud other than credit card fraud, including “compromised lines of credit,
3 internet accounts (e.g., eBay, Amazon) and email payment accounts such as PayPal.”

4 6. Plaintiffs bring this action to remedy these harms on behalf of themselves
5 and all similarly situated individuals whose PII was accessed during the Data Breach.
6 Plaintiffs seek the following remedies, among others: statutory damages under the Fair
7 Credit Reporting Act (“FCRA”) and state consumer protection statutes, reimbursement
8 of out-of-pocket losses, other compensatory damages, further and more robust credit
9 monitoring services with accompanying identity theft insurance beyond Experian’s
10 current two-year offer, and injunctive relief including an order requiring Experian to
11 implement improved data security measures.

12 **PARTIES**

13 **A. Plaintiffs**

14 **Alabama**

15 7. Plaintiff Stephen Allen is a resident of Midland City, Alabama and was an
16 Alabama resident during the period of the Data Breach. Plaintiff Allen applied for a T-
17 Mobile account in Alabama between September 1, 2013 and September 16, 2015 by
18 providing his PII and payment card information. On or about October 10, 2015,
19 Plaintiff Allen received a notification letter from Experian regarding the Data Breach.
20 As a result of the Data Breach, Plaintiff Allen has spent over 18 hours addressing issues
21 arising from the Data Breach, including monitoring his bank accounts and credit report
22 for fraudulent activity.

23 **Arizona**

24 8. Plaintiff Richard Parks is a resident of Arizona City, Arizona and was an
25 Arizona resident during the period of the Data Breach. Plaintiff Parks applied for an
26 upgraded T-Mobile account in Arizona between September 1, 2013 and September 16,
27 2015 by providing his PII, and has been a T-Mobile customer since 2004. On or about
28 October 13, 2015, Plaintiff Parks received a notification letter from Experian regarding

1 the Data Breach. On or about October 15, 2015, Plaintiff Parks received a suspicious
2 account statement from the Social Security Administration (“SSA”) that bore his
3 mailing address but another person’s name. Mr. Parks returned the letter to the SSA,
4 along with a cover letter explaining that he was not the person on the addressee line.
5 His letter asked the SSA to investigate for possible fraud. As a result of the Data
6 Breach, Plaintiff Parks paid for credit freezes to be applied to his credit report, which
7 have cost him approximately \$48 to date (including certified mail fees and money order
8 fees) and have not been reimbursed. Plaintiff Parks also filed a police report, and sent
9 numerous letters and/or identity theft forms to his banks, the Federal Trade
10 Commission, the Internal Revenue Service, and several other entities informing them of
11 the breach and his resulting risk of identity theft. He incurred out-of-pocket costs for
12 postage for mailing these letters. Plaintiff Parks has spent approximately 40 hours
13 addressing issues arising from the Data Breach, including addressing the suspicious
14 activity and monitoring his bank accounts and credit report for fraudulent activity.

15 9. Plaintiff Ryan Hamre is a resident of Phoenix, Arizona and was an Arizona
16 resident during the period of the Data Breach. Plaintiff Hamre applied for a T-Mobile
17 account in Arizona between September 1, 2013 and September 16, 2015 by providing
18 his PII and payment card information, and has been a T-Mobile customer since
19 February 21, 2014. In or around October 2015, Plaintiff Hamre received a notification
20 letter from Experian regarding the Data Breach. As a result of the Data Breach, Plaintiff
21 Hamre has spent over 10 hours addressing issues arising from the Data Breach,
22 including monitoring his bank accounts and credit report for fraudulent activity.

23 **California**

24 10. Plaintiff Joshua Gonzales is a resident of San Diego, California and was a
25 California resident during the period of the Data Breach. Plaintiff Gonzales applied for
26 a T-Mobile account in California between September 1, 2013 and September 16, 2015
27 by providing his PII and payment card information, and was a T-Mobile customer from
28 2014 to 2015. In or around October 2015, Plaintiff Gonzales received a notification

1 letter from Experian regarding the Data Breach. In or around December 2015, Plaintiff
2 Gonzales attempted to purchase a vehicle and discovered several hard inquiries on his
3 credit report, which had caused his credit score to drop approximately 30 points.
4 Plaintiff Gonzales is still attempting to resolve these fraudulent credit inquiries and
5 anticipates having to spend thousands of dollars to hire someone to repair his credit. As
6 a result of the Data Breach, Plaintiff Gonzales paid to obtain credit reports from all three
7 bureaus, which have cost him approximately \$30 to date and have not been reimbursed.
8 Plaintiff Gonzales incurred unreimbursed expenses and has spent over 40 hours
9 addressing issues arising from the Data Breach, including addressing the fraudulent
10 activity and monitoring his financial accounts and credit report.

11 11. Plaintiff Gwendolyn Crump is a resident of Los Angeles, California and
12 was a California resident during the period of the Data Breach. Plaintiff Crump applied
13 for T-Mobile services in California between September 1, 2013 and September 16, 2015
14 by providing her PII and payment card information, and was a T-Mobile customer from
15 2008 to 2014. In or around April 2015, Plaintiff Crump was notified that someone
16 attempted to impersonate her to obtain a fraudulent T-Mobile account. Plaintiff Crump
17 is still attempting to resolve this identity theft, which resulted in a hard inquiry on her
18 credit report. As a result of the Data Breach, Plaintiff Crump has spent over 10 hours
19 addressing issues arising from the Data Breach, including addressing the fraudulent
20 activity and monitoring her financial accounts and credit report. Plaintiff Crump never
21 received a notification letter from Experian regarding the Data Breach.

22 12. Plaintiff Elleen Brazzle is a resident of Santa Clarita, California and was a
23 California resident during the period of the Data Breach. Plaintiff Brazzle applied for a
24 T-Mobile account in California between September 1, 2013 and September 16, 2015 by
25 providing her PII and payment card information, and has been a T-Mobile customer
26 since February 25, 2014. In or around October 2015, Plaintiff Brazzle received a
27 notification letter from Experian regarding the Data Breach. In or around November
28 2015, Plaintiff Brazzle's bank notified her of over \$100 in fraudulent charges on her

1 debit card associated with her primary checking account. Although she accepted
2 Experian's free credit monitoring offer, Experian's credit monitoring service did not
3 notify Plaintiff Brazzle of the fraudulent activity. Plaintiff Brazzle took time off work
4 to resolve these fraudulent charges and obtain reimbursement, losing over \$1,000 in
5 wages. As a result of the Data Breach, Plaintiff Brazzle has spent over 40 hours
6 addressing issues arising from the Data Breach, including resolving the fraudulent
7 charges and checking her accounts for additional fraud.

8 13. Plaintiff Melissa Merry is a resident of Long Beach, California and was a
9 California resident during the period of the Data Breach. Plaintiff Merry applied for a
10 T-Mobile account in California between September 1, 2013 and September 16, 2015 by
11 providing her PII and payment card information, and has been a T-Mobile customer
12 since April 2015. On or about October 13, 2015, Plaintiff Merry received a notification
13 letter from Experian regarding the Data Breach. On or about January 8, 2016, Plaintiff
14 Merry attempted to withdraw cash from her primary checking account and was unable
15 to make the withdrawal. After contacting her bank, Plaintiff Merry discovered that a
16 fraudulent withdrawal was attempted on her account and it had been frozen. During the
17 three weeks it took for her replacement debit card to arrive, Plaintiff Merry had to make
18 additional trips to the bank to withdraw cash. As a result of the Data Breach, Plaintiff
19 Merry has spent over 20 hours addressing issues arising from the Data Breach,
20 including resolving the fraudulent activity and checking her accounts for additional
21 fraud.

22 14. Plaintiff Francisco Ojeda is a resident of San Jose, California and was a
23 California resident during the period of the Data Breach. Plaintiff Ojeda applied for a
24 T-Mobile account in California between September 1, 2013 and September 16, 2015 by
25 providing his PII and payment card information, and has been a T-Mobile customer
26 since January 2015. In or around November 2015, Plaintiff Ojeda discovered
27 unauthorized charges on his bank statement and he is attempting to resolve these
28 charges. As a result of the Data Breach, Plaintiff Ojeda has spent over five hours

1 addressing issues arising from the Data Breach, including resolving the fraudulent
2 activity and checking his accounts for additional fraud. Plaintiff Ojeda never received a
3 notification letter from Experian regarding the Data Breach.

4 15. Plaintiff Nora Bohannon is a resident of Fairfield, California and was a
5 California resident during the period of the Data Breach. Plaintiff Bohannon applied for
6 a T-Mobile account in California between September 1, 2013 and September 16, 2015
7 by providing his PII and payment card information, and has been a T-Mobile customer
8 since 2013. In or around October 2015, Plaintiff Bohannon received a notification letter
9 from Experian regarding the Data Breach. In or around November 2015, Plaintiff
10 Bohannon began receiving calls that someone was attempting to use his PII to open
11 lines of credit at banks and retail stores. These fraudulent account attempts, at about 10
12 banks and 15 stores, have shown up as inquiries on his credit report and affected his
13 credit score. In or around December 2015, Plaintiff Bohannon suffered a fraudulent
14 charge of approximately \$800 for bitcoins on his checking account. In or around
15 February 2016, police notified Plaintiff Bohannon that they had arrested an individual
16 carrying three fraudulent credit cards opened in his name. As a result of the Data
17 Breach, Plaintiff Bohannon has spent over 80 hours addressing issues arising from the
18 Data Breach, including resolving the fraudulent activity and checking his accounts and
19 credit report for fraud.

20 16. Plaintiffs Gregory and Kashia Johnson are residents of Lompoc, California
21 and were California residents during the period of the Data Breach. The Johnson
22 Plaintiffs applied for T-Mobile accounts in California between September 1, 2013 and
23 September 16, 2015 by providing their PII and payment card information, and have
24 been T-Mobile customers since 2013. In or around October 2015, the Johnson Plaintiffs
25 received a notification letter from Experian regarding the Data Breach. Also in or
26 around October 2015, Mr. Johnson received a call from their bank indicating that
27 someone had run his credit outside of California and advising him to place a 90-day
28 fraud alert on his credit report. Mr. Johnson followed this advice and placed an alert on

1 his credit report. As a result of the Data Breach, the Johnson Plaintiffs have spent over
2 five hours addressing issues arising from the Data Breach, including resolving the
3 fraudulent activity and checking their accounts and credit reports for fraud.

4 17. Plaintiff David Ciano is a resident of San Luis Obispo, California and was
5 a California resident during the period of the Data Breach. Plaintiff Ciano applied for a
6 T-Mobile account in California between September 1, 2013 and September 16, 2015 by
7 providing his PII and payment card information, and has been a T-Mobile customer
8 since December 2013. On or about October 13, 2015, Plaintiff Ciano received a
9 notification letter from Experian regarding the Data Breach. As a result of the Data
10 Breach, Plaintiff Ciano has spent over three hours addressing issues arising from the
11 Data Breach, including checking his accounts for fraud.

12 **Colorado**

13 18. Plaintiff Bradford Daghita is a resident of Wheat Ridge, Colorado and was
14 a Colorado resident during the period of the Data Breach. Plaintiff Daghita applied for
15 a T-Mobile account in Colorado between September 1, 2013 and September 16, 2015 by
16 providing his PII and payment card information, and has been a T-Mobile customer
17 since September 2, 2014. On or about October 27, 2015, Plaintiff Daghita received a
18 notification letter from Experian regarding the Data Breach. As a result of the Data
19 Breach, Plaintiff Daghita has spent about \$300 on an annual credit monitoring service
20 and spent over five hours addressing issues arising from the Data Breach, including
21 checking his accounts and credit report for fraud.

22 **Delaware**

23 19. Plaintiff Alison Cochran is a resident of Newark, Delaware and was a
24 Delaware resident during the period of the Data Breach. Plaintiff Cochran applied for
25 T-Mobile services in Delaware between September 1, 2013 and September 16, 2015 by
26 providing her PII and payment card information, and has been a T-Mobile customer for
27 over a decade. On or about September 9, 2015, Plaintiff Cochran's mobile device
28 stopped working. She contacted T-Mobile, who informed her that her phone was

1 reported stolen and had been deactivated. Whoever fraudulently reported the stolen
2 phone had her name, address, Social Security number, and account information.
3 Plaintiff Cochran had to file four different fraud claims with T-Mobile to get this issue
4 resolved. In or around October 2015, Plaintiff Cochran received a notification letter
5 from Experian regarding the Data Breach. As a result of the Data Breach, Plaintiff
6 Cochran has spent over 20 hours addressing issues arising from the Data Breach,
7 including resolving the fraudulent activity and checking her accounts for additional
8 fraud.

9 **District of Columbia**

10 20. Plaintiff Alice Dunscomb is a resident of Washington, DC and was a
11 District of Columbia resident during the period of the Data Breach. Plaintiff Dunscomb
12 applied for a T-Mobile account in the District of Columbia between September 1, 2013
13 and September 16, 2015 by providing her PII and payment card information, and has
14 been a T-Mobile customer since 2013. In or around October 2015, Plaintiff Dunscomb
15 received a notification letter from Experian regarding the Data Breach. As a result of
16 the Data Breach, Plaintiff Dunscomb has spent \$20 to freeze her credit report and spent
17 over six hours addressing issues arising from the Data Breach, including checking her
18 accounts and credit report for fraud.

19 **Florida**

20 21. Plaintiff Jessica Holt is a resident of Lehigh Acres, Florida and was a
21 Florida resident during the period of the Data Breach. Plaintiff Holt applied for a T-
22 Mobile account in Florida between September 1, 2013 and September 16, 2015 by
23 providing her PII and payment card information, and has been a T-Mobile customer
24 since July 2015. In the summer of 2015, Plaintiff Holt's debit card was fraudulently
25 used to purchase approximately \$150 worth of merchandise online. In or around
26 October 2015, Plaintiff Holt received a notification letter from Experian regarding the
27 Data Breach. As a result of the Data Breach, Plaintiff Holt has spent over 20 hours
28 addressing issues arising from the Data Breach, including resolving the fraudulent

1 activity and checking her accounts for additional fraud.

2 22. Plaintiff Samantha Manganaris is a resident of Jacksonville Beach, Florida
3 and was a Florida resident during the period of the Data Breach. Plaintiff Manganaris
4 applied for a T-Mobile account in Florida between September 1, 2013 and September
5 16, 2015 by providing her PII and payment card information. In or around December
6 2014, Plaintiff Manganaris experienced fraudulent activity on her bank account, which
7 was ultimately reimbursed. Around the same time, she began receiving threatening
8 phishing calls every week from an individual that knew her date of birth and bank
9 account information, and said there was a warrant out for her arrest. In or around
10 October 2015, Plaintiff Manganaris received a notification letter from Experian
11 regarding the Data Breach. As a result of the Data Breach, Plaintiff Manganaris has
12 spent over 20 hours addressing issues arising from the Data Breach, including resolving
13 the fraudulent activity and checking her accounts for additional fraud.

14 23. Plaintiff Veronica Gillotte is a resident of Boca Raton, Florida and was a
15 Florida resident during the period of the Data Breach. Plaintiff Gillotte applied for a T-
16 Mobile account in Florida between September 1, 2013 and September 16, 2015 by
17 providing her PII and payment card information, and has been a T-Mobile customer
18 since 2013. In or around September 2015, Plaintiff Gillotte received a notification letter
19 from Experian regarding the Data Breach. In or around December 2015, Plaintiff
20 Gillotte received a phishing call from someone claiming to be a local clerk of court and
21 that she owed the court \$2,700. The caller already had Plaintiff Gillotte's name and
22 Social Security Number. After contacting the actual clerk of court and determining the
23 call was a scam, Plaintiff Gillotte had to cancel her bank account and open a new
24 account. Also within the last six months, someone cancelled her debit card twice and
25 Plaintiff Gillotte received replacement debit cards without having requested them. The
26 same scammer called back in January and February 2016 demanding the \$2,700
27 payment. As a result of the Data Breach, Plaintiff Gillotte has spent over 8 hours
28 addressing issues arising from the Data Breach, including resolving the fraudulent

1 activity and checking her accounts for fraud.

2 24. Plaintiff David Brown is a resident of Jupiter, Florida and was a Florida
3 resident during the period of the Data Breach. Plaintiff Brown applied for a T-Mobile
4 account in Florida between September 1, 2013 and September 16, 2015 by providing his
5 PII and payment card information, and has been a T-Mobile customer since 2014. On
6 or about October 8, 2015, Plaintiff Brown received a notification letter from Experian
7 regarding the Data Breach. On October 10, 2015, an identity thief purchased two Apple
8 iPhones in his name from a Verizon store, totaling \$1,698. The thief purchased the
9 phones in-person using Mr. Brown's personal information. Verizon eventually reversed
10 the fraudulent charges. Mr. Brown had never experienced identity theft prior to the
11 Experian breach. As a result of the Data Breach, Plaintiff Brown has spent over eight
12 hours addressing issues arising from the Data Breach, including addressing the
13 fraudulent activity and checking his accounts for fraud and placing a credit freeze on his
14 credit report.

15 25. Plaintiff Stuart Zimmelman is a resident of Wellington, Florida and was a
16 Florida resident during the period of the Data Breach. Plaintiff Zimmelman applied for
17 T-Mobile services in Florida between September 1, 2013 and September 16, 2015 by
18 providing his PII and payment card information, and has been a T-Mobile customer
19 since 2010. As a result of the Data Breach, Plaintiff Zimmelman has spent three hours
20 addressing issues arising from the Data Breach, including checking his accounts for
21 fraud. Plaintiff Zimmelman never received a notification letter from Experian regarding
22 the Data Breach.

23 26. Plaintiff Chris Shearer is a resident of St. Augustine, Florida and was a
24 Florida resident during the period of the Data Breach. Plaintiff Shearer applied for a T-
25 Mobile account in Florida between September 1, 2013 and September 16, 2015 by
26 providing his PII and payment card information. In or around October 2015, Plaintiff
27 Shearer received a notification letter from Experian regarding the Data Breach. As a
28 result of the Data Breach, Plaintiff Shearer has spent about ten hours addressing issues

1 arising from the Data Breach, including checking his accounts for fraud.

2 **Georgia**

3 27. Plaintiff Christiaan Mealey is a resident of Atlanta, Georgia and was a
4 Georgia resident during the period of the Data Breach. Plaintiff Mealey applied for a T-
5 Mobile account in Georgia between September 1, 2013 and September 16, 2015 by
6 providing his PII and payment card information, and has been a T-Mobile customer
7 since 2014. In or around October 2015, Plaintiff Mealey received a notification letter
8 from Experian regarding the Data Breach. As a result of the Data Breach, Plaintiff
9 Mealey has spent about \$75 on credit monitoring and spent over 20 hours addressing
10 issues arising from the Data Breach, including checking his accounts and credit report
11 for fraud.

12 28. Plaintiff Gregory Hertik is a resident of Cumming, Georgia and was a
13 Georgia resident during the period of the Data Breach. Plaintiff Hertik applied for a T-
14 Mobile account in Georgia between September 1, 2013 and September 16, 2015 by
15 providing his PII and payment card information. On or about October 29, 2015,
16 Plaintiff Hertik received a notification letter from Experian regarding the Data Breach.
17 As a result of the Data Breach, Plaintiff Hertik has spent about \$50 on monthly credit
18 monitoring and spent over three hours addressing issues arising from the Data Breach,
19 including checking his accounts and credit report for fraud.

20 **Hawaii**

21 29. Plaintiff Allan Sommercorn is a resident of Kaaawa, Hawaii and was a
22 Hawaii resident during the period of the Data Breach. Plaintiff Sommercorn applied for
23 T-Mobile services in Hawaii between September 1, 2013 and September 16, 2015 by
24 providing his PII and payment card information, and has been a T-Mobile customer for
25 over a decade. On or about October 18, 2015, Plaintiff Sommercorn received a
26 notification letter from Experian regarding the Data Breach. In or around November
27 2015, Plaintiff Sommercorn suffered two unauthorized charges on his credit card and
28 began receiving fraudulent debt collection calls. As a result of the Data Breach,

1 Plaintiff Sommercorn has spent over 20 hours addressing issues arising from the Data
2 Breach, including addressing the fraudulent activity and checking his accounts and
3 credit report for fraud.

4 **Illinois**

5 30. Plaintiff Kamil Kuklinski is a resident of Bartlett, Illinois and was an
6 Illinois resident during the period of the Data Breach. Plaintiff Kuklinski applied for a
7 T-Mobile account in Illinois between September 1, 2013 and September 16, 2015 by
8 providing his PII and payment card information, and has been a T-Mobile customer
9 since April 2014. On or about September 13, 2015, Plaintiff Kuklinski received
10 disturbing text messages from an apparent hacker stating that payment of over \$3,000
11 was due for an account that was not his own. When Plaintiff Kuklinski challenged the
12 charges, the hacker threatened him with 500 more text messages and mentioned his
13 girlfriend by name, who was the primary account holder on his T-Mobile service. On or
14 about October 5, 2015, Plaintiff Kuklinski received a notification letter from Experian
15 regarding the Data Breach. In or about March 2016, Plaintiff Kuklinski received a letter
16 from the IRS informing him that their electronic security filters had detected a
17 suspicious, but ultimately unsuccessful, attempt to use his Social Security number to file
18 a fraudulent tax return. As a result of the Data Breach, Plaintiff Kuklinski has spent
19 over eight hours addressing issues arising from the Data Breach, including addressing
20 the fraudulent activity and checking his accounts and credit report for fraud.

21 31. Plaintiff Charles Yoo is a resident of Kildeer, Illinois and was an Illinois
22 resident during the period of the Data Breach. Plaintiff Yoo applied for a T-Mobile
23 account in Illinois between September 1, 2013 and September 16, 2015 by providing his
24 PII and payment card information, and has been a T-Mobile customer since October 1,
25 2014. On or about October 7, 2015, Plaintiff Yoo received a notification letter from
26 Experian regarding the Data Breach. In or around November 2015, Plaintiff Yoo's bank
27 informed him of attempted fraudulent charges on his credit card. As a result of the Data
28 Breach, Plaintiff Yoo has spent over three hours addressing issues arising from the Data

1 Breach, including addressing the fraudulent activity and checking his accounts and
2 credit report for fraud.

3 32. Plaintiff Sergey Barbashov is a resident of Plainfield, Illinois and was an
4 Illinois resident during the period of the Data Breach. Plaintiff Barbashov applied for a
5 T-Mobile account in Illinois between September 1, 2013 and September 16, 2015 by
6 providing his PII and payment card information. In or around October 2015, Plaintiff
7 Barbashov received a notification email from Experian regarding the Data Breach. As a
8 result of the Data Breach, Plaintiff Barbashov has spent approximately two hours
9 addressing issues arising from the Data Breach, including checking his accounts and
10 credit report for fraud.

11 33. Plaintiff Kathleen Alcorn is a resident of Springfield, Illinois and was an
12 Illinois resident during the period of the Data Breach. Plaintiff Alcorn applied for a T-
13 Mobile account in Illinois between September 1, 2013 and September 16, 2015 by
14 providing her PII and payment card information, and has been a T-Mobile customer
15 since August 2015. On or about October 12, 2015, Plaintiff Alcorn received a
16 notification letter from Experian regarding the Data Breach. After receiving this
17 notification, Plaintiff Alcorn started a credit monitoring and identity theft protection
18 subscription that costs her about \$27 per month. As a result of the Data Breach,
19 Plaintiff Alcorn has spent about \$108 to date on credit monitoring and spent over 30
20 hours addressing issues arising from the Data Breach, including checking her accounts
21 and credit report for fraud.

22 **Indiana**

23 34. Plaintiff Mary Roberts is a resident of Clinton, Indiana and was an Indiana
24 resident during the period of the Data Breach. Plaintiff Roberts applied for a T-Mobile
25 account in Indiana between September 1, 2013 and September 16, 2015 by providing
26 her PII and payment card information. In or around October 2015, Plaintiff Roberts
27 received a notification letter from Experian regarding the Data Breach. In or around
28 April 2016, Plaintiff Roberts discovered an unauthorized credit inquiry on her credit

1 report, which has not yet been resolved. She also discovered that someone else had
2 obtained her free credit report from one of the credit bureaus without her authorization,
3 so that she was unable to obtain a free copy. As a result of the Data Breach, Plaintiff
4 Roberts has spent about 100 hours addressing issues arising from the Data Breach,
5 including checking her credit report for fraud and researching preventative measures.

6 **Kentucky**

7 35. Plaintiff Tony George is a resident of Columbia, Kentucky and was a
8 Kentucky resident during the period of the Data Breach. Plaintiff George applied for a
9 T-Mobile account in Kentucky between September 1, 2013 and September 16, 2015 by
10 providing his PII and payment card information. On or about October 10, 2015,
11 Plaintiff George received a notification letter from Experian regarding the Data Breach.
12 In or around November 2015, Plaintiff George began receiving suspicious phishing calls
13 and emails, and there was an unauthorized inquiry on his credit report. As a result of
14 the Data Breach, Plaintiff George has spent about 100 hours to date addressing issues
15 arising from the Data Breach, including addressing the fraudulent activity and checking
16 his credit reports for fraud.

17 **Massachusetts**

18 36. Plaintiff Ryan Heitz is a resident of Attleboro, Massachusetts and was a
19 Massachusetts resident during the period of the Data Breach. Plaintiff Heitz applied for
20 a T-Mobile account in Massachusetts between September 1, 2013 and September 16,
21 2015 by providing his PII and payment card information, and has been a T-Mobile
22 customer since April 2015. On or about October 26, 2015, Plaintiff Heitz received a
23 notification letter from Experian regarding the Data Breach. As a result of the Data
24 Breach, Plaintiff Heitz has spent about \$25 to place freezes on his credit report and over
25 20 hours addressing issues arising from the Data Breach, including checking his
26 accounts and credit report for fraud.

27 37. Plaintiff Gerardus Jansen is a Dutch citizen and a resident of Arlington,
28 Massachusetts and was a Massachusetts resident during the period of the Data Breach.

1 Plaintiff Jansen applied for a T-Mobile account in Massachusetts between September 1,
2 2013 and September 16, 2015 by providing his PII and payment card information, and
3 has been a T-Mobile customer since April 29, 2015. In or around October 2015,
4 Plaintiff Jansen received a notification letter from Experian regarding the Data Breach.
5 As a result of the Data Breach, Plaintiff Jansen spends up to one hour per month
6 checking his credit report for fraud.

7 **Michigan**

8 38. Plaintiff Lorenzo Jackson is a resident of Flint, Michigan and was a
9 Michigan resident during the period of the Data Breach. Plaintiff Jackson applied for a
10 T-Mobile account in Michigan between September 1, 2013 and September 16, 2015 by
11 providing his PII and payment card information, and has been a T-Mobile customer
12 since March 2014. In or around October 2015, Plaintiff Jackson received a notification
13 letter from Experian regarding the Data Breach. As a result of the Data Breach, Plaintiff
14 Jackson has spent over two hours addressing issues arising from the Data Breach,
15 including checking his accounts for fraud.

16 **Minnesota**

17 39. Plaintiff Eban Liebig is a resident of Columbia Heights, Minnesota and was
18 a Minnesota resident during the period of the Data Breach. Plaintiff Liebig applied for a
19 T-Mobile account in Minnesota between September 1, 2013 and September 16, 2015 by
20 providing his PII and payment card information, and has been a T-Mobile customer
21 since April 8, 2014. In or around October 2015, Plaintiff Liebig received a notification
22 letter from Experian regarding the Data Breach. As a result of the Data Breach, Plaintiff
23 Liebig has spent \$15 to freeze his credit report and spent over 20 hours addressing
24 issues arising from the Data Breach, including checking his accounts and credit report
25 for fraud.

26 40. Plaintiff Angelia Fennern is a resident of St. Paul, Minnesota and was a
27 Minnesota resident during the period of the Data Breach. Plaintiff Fennern applied for a
28 T-Mobile account in Minnesota between September 1, 2013 and September 16, 2015 by

1 providing her PII and payment card information, and has been a T-Mobile customer
2 since May 2015. On or about October 5, 2015, Plaintiff Fennern received a notification
3 letter from Experian regarding the Data Breach. As a result of the Data Breach, Plaintiff
4 Fennern has spent over five hours addressing issues arising from the Data Breach,
5 including checking her accounts for fraud.

6 **Missouri**

7 41. Plaintiff Charles Sallade is a resident of St. Louis, Missouri and was a
8 Missouri resident during the period of the Data Breach. Plaintiff Sallade applied for a
9 T-Mobile account in Missouri between September 1, 2013 and September 16, 2015 by
10 providing his PII and payment card information, and has been a T-Mobile customer
11 since March 2015. On or about October 15, 2015, Plaintiff Sallade received a
12 notification letter from Experian regarding the Data Breach. He signed up for credit
13 monitoring and identity theft protection, for which he pays \$10 per month. In or around
14 October 2015, his credit monitoring service notified him that someone attempted to
15 open a fraudulent line of credit with his name and Social Security number. As a result
16 of the Data Breach, Plaintiff Sallade has spent \$40 to date on credit monitoring and
17 spent over 20 hours addressing issues arising from the Data Breach, including
18 addressing the fraudulent activity and checking his accounts and credit report for fraud.

19 **Nevada**

20 42. Plaintiff Cregan Smith is a resident of Las Vegas, Nevada and was a
21 Nevada resident during the period of the Data Breach. Plaintiff Smith applied for T-
22 Mobile services in Nevada between September 1, 2013 and September 16, 2015 by
23 providing his PII and payment card information, and has been a T-Mobile customer
24 since 2008. In or around September 2015, someone attempted to open a line of credit in
25 Plaintiff Smith's name. When trying to file his 2015 income tax return, Plaintiff
26 Smith's accountant informed him the return was flagged and could not be filed because
27 he listed his mother as a dependent and a fraudulent return had already been filed with
28 her Social Security number. Plaintiff Smith's anticipated refund was almost \$1,000 less

1 because he was unable to claim his mother as a dependent, an issue that has not yet been
2 resolved with the IRS. In or around February 2016, Plaintiff Smith finally received a
3 notification letter from Experian regarding the Data Breach. As a result of the Data
4 Breach, Plaintiff Smith has spent over 20 hours addressing issues arising from the Data
5 Breach, including mitigating his tax fraud issues and checking his accounts and credit
6 report for fraud.

7 43. Plaintiff Giovanni Williams is a resident of Las Vegas, Nevada and was a
8 Nevada resident during the period of the Data Breach. Plaintiff Williams applied for a
9 T-Mobile account in Nevada between September 1, 2013 and September 16, 2015 by
10 providing his PII and payment card information, and has been a T-Mobile customer
11 since June 3, 2014. In or around October 2015, Plaintiff Williams received a
12 notification letter from Experian regarding the Data Breach. As a result of the Data
13 Breach, Plaintiff Williams has spent approximately 20 hours addressing issues arising
14 from the Data Breach, including checking his accounts and credit report for fraud. In
15 addition, Plaintiff Williams has spent approximately \$140 on credit freezes and credit
16 monitoring protection.

17 **New Jersey**

18 44. Plaintiff Dipak Bhuta is a resident of Voorhees, New Jersey and was a New
19 Jersey resident during the period of the Data Breach. Plaintiff Bhuta applied for a T-
20 Mobile account in New Jersey between September 1, 2013 and September 16, 2015 by
21 providing his PII and payment card information, and has been a T-Mobile customer
22 since November 2014. On or about October 5, 2015, Plaintiff Bhuta received a
23 notification letter from Experian regarding the Data Breach. After learning of the Data
24 Breach, Plaintiff Bhuta purchased annual credit monitoring for approximately \$120. As
25 a result of the Data Breach, Plaintiff Bhuta has spent over two hours addressing issues
26 arising from the Data Breach, including checking his accounts for fraud.

27 45. Plaintiff Joseph Zubrzycki is a resident of Blackwood, New Jersey and was
28 a New Jersey resident during the period of the Data Breach. Plaintiff Zubrzycki applied

1 for T-Mobile services in New Jersey between September 1, 2013 and September 16,
2 2015 by providing his PII and payment card information, and has been a T-Mobile
3 customer since approximately 2010. In or around October 2015, Plaintiff Zubrzycki
4 received a notification letter from Experian regarding the Data Breach. Earlier in 2015,
5 Plaintiff Zubrzycki received a letter from the IRS indicating that someone tried to
6 fraudulently access his IRS account information but the IRS blocked the attempt. In
7 early 2016, Plaintiff Zubrzycki received a letter from an online vendor requesting his
8 credit card information for an account that he did not open. In addition, he recently
9 learned that someone fraudulently obtained his annual free credit reports from all three
10 credit bureaus. As a result of the Data Breach, Plaintiff Zubrzycki has spent
11 approximately \$7 to obtain his credit score and over two hours addressing issues arising
12 from the Data Breach, including checking his accounts and credit report for fraud.

13 **New Mexico**

14 46. Plaintiff Lucio Hernandez is a resident of Los Lunas, New Mexico and was
15 a New Mexico resident during the period of the Data Breach. Plaintiff Hernandez
16 applied for a T-Mobile account in New Mexico between September 1, 2013 and
17 September 16, 2015 by providing his PII and payment card information. On or about
18 October 8, 2015, Plaintiff Hernandez received a notification letter from Experian
19 regarding the Data Breach. A few months later, Plaintiff Hernandez discovered an
20 individual using his identity on the Internet, including information about his family
21 members. On or about March 28, 2016, Plaintiff Hernandez received a letter from a
22 telephone provider about a past due invoice of about \$400 despite not having any
23 account with that provider. As a result of the Data Breach, Plaintiff Hernandez has
24 spent about \$17 to investigate the online identity theft and over 10 hours addressing
25 issues arising from the Data Breach, including addressing the fraudulent activity and
26 checking his accounts and credit report for fraud.

27 **New York**

28 47. Plaintiff Shivan Bassaw is a resident of Bronx, New York and was a New

1 York resident during the period of the Data Breach. Plaintiff Bassaw applied for a T-
2 Mobile account in New York between September 1, 2013 and September 16, 2015 by
3 providing his PII and payment card information, and has been a T-Mobile customer
4 since September 15, 2013. On or about November 15, 2015, Plaintiff Bassaw's credit
5 card had an unauthorized charge that was ultimately reimbursed. As a result of the Data
6 Breach, Plaintiff Bassaw has spent approximately 3 hours addressing issues arising from
7 the Data Breach, including addressing the fraudulent activity and checking his accounts
8 and credit report for fraud.

9 **North Carolina**

10 48. Plaintiff Jennifer Looney is a resident of Charlotte, North Carolina and was
11 a North Carolina resident during the period of the Data Breach. Plaintiff Looney
12 applied for a T-Mobile account in North Carolina between September 1, 2013 and
13 September 16, 2015 by providing her PII and payment card information. Beginning in
14 or around September 2015, Plaintiff Looney began receiving email notifications of
15 attempts to connect her email address with another email without her authorization. She
16 reported this unauthorized activity to her email provider. In or around October 2015,
17 Plaintiff Looney received a notification letter from Experian regarding the Data Breach.
18 As a result of the Data Breach, Plaintiff Looney has spent approximately \$20 per month
19 on credit monitoring and spent over 80 hours addressing issues arising from the Data
20 Breach, including addressing the fraudulent activity, placing freezes on her credit report
21 with all three credit bureaus, and checking her accounts and credit report for fraud.

22 **Ohio**

23 49. Plaintiff Darius Clark is a resident of Cincinnati, Ohio and was an Ohio
24 resident during the period of the Data Breach. Plaintiff Clark applied for a T-Mobile
25 account in Ohio between September 1, 2013 and September 16, 2015 by providing his
26 PII and payment card information. In or around September 2015, Plaintiff Clark
27 received several phishing calls in which the caller knew his mailing address and the last
28 four digits of his Social Security number and claimed Plaintiff Clark owed taxes to the

1 IRS. Plaintiff Clark later confirmed with the IRS that he did not owe any taxes and
2 these were fraudulent phishing calls. Ultimately, Plaintiff Clark changed his telephone
3 number to avoid these calls. On or about October 26, 2015, Plaintiff Clark received a
4 notification letter from Experian regarding the Data Breach. After the Data Breach,
5 Plaintiff Clark has spent approximately \$20 placing credit freezes on his credit report,
6 and approximately \$20 per month on credit monitoring. Also a result of the Data
7 Breach, Plaintiff Clark has spent over 100 hours addressing issues arising from the Data
8 Breach, including contacting the IRS, and checking his accounts and credit report for
9 fraud.

10 **Oregon**

11 50. Plaintiff Hunter Graham is a resident of Portland, Oregon and was an
12 Oregon resident during the period of the Data Breach. Plaintiff Graham applied for a T-
13 Mobile account in Oregon between September 1, 2013 and September 16, 2015 by
14 providing his PII and payment card information, and has been a T-Mobile customer
15 since September 2014. On or about October 5, 2015, Plaintiff Graham received a
16 notification letter from Experian regarding the Data Breach. In or around April 2015,
17 Plaintiff Graham learned that someone filed a fraudulent income tax return using his
18 name and Social Security number. The criminal had also opened a fraudulent Turbo
19 Tax account in Plaintiff Graham's name to file the fraudulent return in January 2015.
20 Plaintiff Graham's tax refund of over \$6,000 was delayed for nine months. As a result
21 of the Data Breach, Plaintiff Graham has spent over 40 hours addressing issues arising
22 from the Data Breach, including addressing the fraudulent activity, and checking his
23 accounts and credit report for fraud.

24 51. Plaintiff Philip Popiel is a resident of Beaverton, Oregon and was an
25 Oregon resident during the period of the Data Breach. Plaintiff Popiel applied for a T-
26 Mobile account in Oregon between September 1, 2013 and September 16, 2015 by
27 providing his PII and payment card information. On or about October 15, 2015,
28 Plaintiff Popiel received a notification letter from Experian regarding the Data Breach.

1 As a result of the Data Breach, Plaintiff Popiel has spent about \$30 placing credit
2 freezes on his credit report and over four hours addressing issues arising from the Data
3 Breach, including checking his accounts and credit report for fraud.

4 **Pennsylvania**

5 52. Plaintiff John Reiser is a resident of Pittsburgh, Pennsylvania and was a
6 Pennsylvania resident during the period of the Data Breach. Plaintiff Reiser applied for
7 a T-Mobile account in Pennsylvania between September 1, 2013 and September 16,
8 2015 by providing his PII and payment card information, and has been a T-Mobile
9 customer since February 16, 2014. On or about October 5, 2015, Plaintiff Reiser
10 received a notification letter from Experian regarding the Data Breach. On or about
11 February 19, 2016, Plaintiff Reiser's bank notified him of an attempted fraudulent
12 charge on his credit card, shutting down that line of credit and issuing a replacement
13 card. As a result of the Data Breach, Plaintiff Reiser has spent approximately two hours
14 addressing issues arising from the Data Breach, including checking his accounts for
15 additional fraud.

16 53. Plaintiff Jennifer Brandabur is a resident of Elkins Park, Pennsylvania and
17 was a Pennsylvania resident during the period of the Data Breach. Plaintiff Brandabur
18 applied for a T-Mobile account in Pennsylvania between September 1, 2013 and
19 September 16, 2015 by providing her PII and payment card information, and has been a
20 T-Mobile customer since June 19, 2015. On or about October 26, 2015, Plaintiff
21 Brandabur received a notification letter from Experian regarding the Data Breach. In or
22 around November 2015, Plaintiff Brandabur's bank notified her of fraudulent charges
23 on her credit card totaling about \$1,000. Approximately \$500 of these fraudulent
24 charges has not been resolved or reimbursed to date. As a result of the Data Breach,
25 Plaintiff Brandabur has spent over four hours addressing issues arising from the Data
26 Breach, including checking her accounts for additional fraud.

27 **South Carolina**

28 54. Plaintiff Perry Heath is a resident of Rockhill, South Carolina and was a

1 South Carolina resident during the period of the Data Breach. Plaintiff Heath applied
2 for a T-Mobile account in South Carolina between September 1, 2013 and September
3 16, 2015 by providing his PII and payment card information, and has been a T-Mobile
4 customer since 2014. In or around October 2015, Plaintiff Heath received a notification
5 letter from Experian regarding the Data Breach. Plaintiff Heath's bank later notified
6 him that someone used his account information to make fraudulent purchases of almost
7 \$300, which caused about four overdraft fees on his account for \$35 each. Ultimately,
8 Plaintiff Heath closed that bank account and opened a new one, but was not reimbursed
9 for the fraudulent charges or overdraft fees. In or around April 2016, Plaintiff Heath
10 attempted to sign up for an internet service but was informed that his PII had already
11 been used to set up an account. As a result of the Data Breach, Plaintiff Heath has lost
12 over \$400 and spent about 40 hours addressing issues arising from the Data Breach,
13 including addressing the fraudulent activity and checking his accounts for fraud.

14 **Tennessee**

15 55. Plaintiff David Lumb is a resident of Memphis, Tennessee and was a
16 Tennessee resident during the period of the Data Breach. Plaintiff Lumb applied for a
17 T-Mobile account in Tennessee between September 1, 2013 and September 16, 2015 by
18 providing his PII and payment card information, and has been a T-Mobile customer
19 since December 2013. On or about November 25, 2015, Plaintiff Lumb received a
20 notification letter from Experian regarding the Data Breach. As a result of the Data
21 Breach, Plaintiff Lumb has spent approximately \$15 placing credit freezes on his credit
22 report and spent over three hours addressing issues arising from the Data Breach,
23 including checking his credit report for fraud.

24 **Texas**

25 56. Plaintiff Martha Cebrian-Vega is a resident of Fort Worth, Texas and was a
26 Texas resident during the period of the Data Breach. Plaintiff Cebrian-Vega applied for
27 a T-Mobile account in Texas between September 1, 2013 and September 16, 2015 by
28 providing her PII and payment card information, and has been a T-Mobile customer

1 since 2014. On or about September 18, 2015, Plaintiff Cebrian-Vega received a letter
2 from a bank that someone had applied for a line of credit in her name. She had to go to
3 the bank to cancel the fraudulent account and file a police report. In or around October
4 2015, Plaintiff Cebrian-Vega received a notification letter from Experian regarding the
5 Data Breach. Plaintiff Cebrian-Vega has started a credit monitoring and identity theft
6 protection subscription that costs her about \$32 per month. As a result of the Data
7 Breach, Plaintiff Cebrian-Vega has spent about 30 hours addressing issues arising from
8 the Data Breach, including addressing the fraudulent activity and checking her accounts
9 and credit report for fraud.

10 **Utah**

11 57. Plaintiffs Mark and Daisy Hodson are residents of Holladay, Utah and were
12 Utah residents during the period of the Data Breach. The Hodson Plaintiffs applied for
13 T-Mobile accounts in Utah between September 1, 2013 and September 16, 2015 by
14 providing their PII and payment card information, and have been T-Mobile customers
15 since March 11, 2015. In or around October 2015, the Hodson Plaintiffs received a
16 notification letter from Experian regarding the Data Breach. Around the same time, the
17 Hodson Plaintiffs had two unauthorized charges on their bank account, which were
18 ultimately reimbursed and replacement debit cards were issued. Also around the same
19 time in October 2015, the Hodson Plaintiffs began receiving frequent phishing calls and
20 emails, which they had not received prior to that time. Mr. Hodson actually had to
21 change his email address to avoid the constant phishing emails. While Mr. Hodson
22 stopped receiving phishing calls in or around February 2016, Mrs. Hodson continues to
23 receive about three per day. As a result of the Data Breach, the Hodson Plaintiffs have
24 spent over 30 hours addressing issues arising from the Data Breach, including resolving
25 the fraudulent activity and checking their accounts and credit reports for fraud.

26 **Virginia**

27 58. Plaintiff Amjed Ababseh is a resident of Christianburg, Virginia and was a
28 Virginia resident during the period of the Data Breach. Plaintiff Ababseh applied for a

1 T-Mobile account in Washington between September 1, 2013 and September 16, 2015
2 by providing his PII and payment card information. In or around October 2015,
3 Plaintiff Ababseh received a notification letter from Experian regarding the Data
4 Breach. In or around November 2015, Plaintiff Ababseh received a notification from
5 his email provider that there was a fraudulent attempt to access his email account in
6 New Orleans, Louisiana. As a result of the Data Breach, Plaintiff Ababseh has spent
7 about \$120 in monthly credit monitoring and over 60 hours addressing issues arising
8 from the Data Breach, including addressing the fraudulent activity and checking his
9 accounts and credit report for fraud.

10 **Washington**

11 59. Plaintiff Martha Schroeder is a resident of Seattle, Washington and was a
12 Washington resident during the period of the Data Breach. Plaintiff Schroeder applied
13 for a T-Mobile account in Washington between September 1, 2013 and September 16,
14 2015 by providing her PII and payment card information, and has been a T-Mobile
15 customer since September 12, 2015. In or around October 2015, Plaintiff Schroeder
16 received a notification letter from Experian regarding the Data Breach. As a result of the
17 Data Breach, Plaintiff Schroeder has spent over 19 hours addressing issues arising from
18 the Data Breach, including checking her accounts and credit report for fraud and placing
19 credit freezes, and has continued to pay \$13 per month for a credit monitoring
20 subscription.

21 60. Plaintiff Jason Shafer is a resident of Vancouver, Washington and was a
22 Washington resident during the period of the Data Breach. Plaintiff Shafer applied for
23 T-Mobile services in Washington between September 1, 2013 and September 16, 2015
24 by providing his PII and payment card information, and has been a T-Mobile customer
25 since April 2013. On or about October 5, 2015, Plaintiff Shafer received a notification
26 letter from Experian regarding the Data Breach. In or around November 2015, Plaintiff
27 Shafer's credit card was declined when he attempted to make a purchase. Plaintiff
28 Shafer's bank informed him that a fraudulent charge was made online and the card was

1 then cancelled and a replacement card was issued. In or around December 2015,
2 Plaintiff Shafer received a letter from his bank indicating he had changed his address
3 when he had not moved or requested any change. Consequently, he cancelled his debit
4 card and another replacement card was issued. As a result of the Data Breach, Plaintiff
5 Shafer has spent over three hours addressing issues arising from the Data Breach,
6 including addressing the fraudulent activity and checking his accounts for fraud.

7 61. Plaintiff Nathaniel Apan is a resident of Florissant, Washington and was a
8 Washington resident during the period of the Data Breach. Plaintiff Apan applied for a
9 T-Mobile account in Washington between September 1, 2013 and September 16, 2015
10 by providing his PII and payment card information. In or around March 2015, Plaintiff
11 Apan discovered a delinquent cellular account on his credit report with about \$400 past
12 due, which he ultimately paid to the provider and was not reimbursed. In or around
13 September 2015, Plaintiff Apan received a bill from another cellular provider for about
14 \$2,000, which he later learned was sent to collections. After reviewing his credit report,
15 he discovered five unauthorized charges from that same provider for about \$4,000 total.
16 Two fraudulent credit card accounts also appeared on his credit report. Plaintiff Apan
17 filed a police report and was able to remove most of the fraudulent activity from his
18 credit report, although at least one unauthorized charge remains outstanding. In or
19 around October 2015, Plaintiff Apan received a notification letter from Experian
20 regarding the Data Breach. In or around November 2015, T-Mobile contacted Plaintiff
21 Apan to inform him that two fraudulent cellular accounts were opened in his name. As
22 a result of the Data Breach, Plaintiff Apan has spent over 50 hours addressing issues
23 arising from the Data Breach, including addressing the fraudulent activity and checking
24 his accounts and credit report for additional fraud.

25 62. Plaintiff Jeffrey Gutschmidt is a resident of Kirkland, Washington and was
26 a Washington resident during the period of the Data Breach. Plaintiff Gutschmidt
27 applied for a T-Mobile account in Washington between September 1, 2013 and
28 September 16, 2015 by providing his PII and payment card information, and has been a

1 T-Mobile customer since January 2014. On or about October 5, 2015, Plaintiff
2 Gutschmidt received a notification letter from Experian regarding the Data Breach. As
3 a result of the Data Breach, Plaintiff Gutschmidt has spent about \$20 to place a credit
4 freeze on his credit report and over 20 hours addressing issues arising from the Data
5 Breach, including checking his accounts for fraud.

6 **B. Defendants**

7 63. Defendant Experian Information Solutions, Inc. is incorporated in Ohio,
8 with its headquarters and principal place of business located at 475 Anton Boulevard,
9 Costa Mesa, CA 92626. It is a citizen of California.

10 64. Defendant Experian Holdings, Inc. is incorporated in Delaware, with its
11 headquarters and principal place of business located at 475 Anton Boulevard, Costa
12 Mesa, CA 92626. It is a citizen of California. Based upon information and belief,
13 Experian Holdings, Inc. is the parent company of Experian Information Solutions, Inc.
14 Experian Holdings, Inc. and Experian Information Solutions, Inc. are referred to
15 collectively as “Experian,” or “Defendants.”

16 65. Experian is one of the major credit reporting bureaus in the United States.
17 As a credit bureau service, Experian is engaged in a number of credit-related services,
18 including “[a]ssisting organizations with evaluating the risks and rewards associated
19 with providing credit to consumers and businesses,” and providing people with “online
20 access to their credit history and score.”⁴ As a credit bureau service, Experian maintains
21 information related to the credit history of consumers and provides the information to
22 credit grantors who are considering a borrower’s application for credit or who have
23 extended credit to the borrower.

24 **JURISDICTION AND VENUE**

25 66. This Court has federal question jurisdiction under 28 U.S.C. § 1331
26 because Plaintiffs are bringing claims under the Fair Credit Reporting Act (“FCRA”),

27
28 ⁴ See *Experian’s Principal Business Groups*, EXPERIAN,
<http://www.experian.com/corporate/principal-businesses.html> (last visited April 14,
2016).

1 15 U.S.C. §§ 1681e, *et seq.*

2 67. This Court also has diversity jurisdiction under the Class Action Fairness
3 Act, 28 U.S.C. § 1332(d), because this is a class action involving more than 100 Class
4 members, the amount in controversy exceeds \$5 million exclusive of interest and costs,
5 and many members of the Class are citizens of states different from Defendants.

6 68. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because
7 Experian is headquartered in this District, it regularly transacts business here, and some
8 of the Class members reside in this District. In addition, the events giving rise to
9 Plaintiffs' causes of action arose, in part, in this District.

10 **FACTS**

11 **A. The Data Breach Compromised the PII of 15 Million Consumers.**

12 69. On October 1, 2015, Experian announced that its systems had been
13 breached and that the Data Breach affected approximately 15 million consumers.
14 According to Experian's press release, unauthorized users acquired the PII of
15 consumers, including T-Mobile customers, from one of Experian's servers. The PII
16 included names, dates of birth, addresses, Social Security numbers, alternative
17 identification numbers, and other personal information:

18
19 Experian North America today announced that one of its
20 business units . . . experienced an unauthorized acquisition of
21 information from a server that contained data on behalf of one
22 of its clients, T-Mobile, USA, Inc. ***The data included some***
23 ***personally identifiable information for approximately 15***
24 ***million consumers in the US***, including those who applied for
25 T-Mobile USA postpaid services or device financing from
26 September 1, 2013 through September 16, 2015

27 . . .
28 ***The data acquired included names, dates of birth, addresses,***
and Social Security numbers and/or an alternative form of

1 *ID like a drivers' license number*, as well as additional
2 information used in T-Mobile's own credit assessment⁵

3 70. On its website, Experian admits the unauthorized disclosure of consumer
4 data and warned consumers of the consequences of the Data Breach:

- 5 • Based on our investigation to date, some organizations had
6 unauthorized disclosure of identifying information and
7 individuals, including some current customers, and also
8 consumers who applied for service or device financing from
9 Sept. 1, 2013 through Sept. 16, 2015, had unauthorized
10 disclosure of their personal information.
- 11 • *The information that was exposed could lead to an increased
12 risk of identity theft.*
- 13 • Be alert to "phishing" by someone who acts like a colleague
14 or friend and requests sensitive information over email, such
15 as passwords, social security numbers, or bank account
16 numbers.
- 17 • Consider placing a fraud alert or security freeze on your credit
18 file.
- 19 • Experian is handling notification about this unauthorized
20 access given that the information was stored on a server in
21 one of our business units.
- 22 • In order to evaluate the risk level of a credit applicant, T-
23 Mobile uses a variety of information to determine the
24 likelihood that a borrower will be able to pay. Information
25 used to do this can include a consumer's payment history, as
26 well as information from Experian or other sources. That

27 ⁵ See Press Release, *Experian Notifies Consumers in the U.S. Who May Have Been*
28 *Affected by Unauthorized Acquisition of a Client's Data*, Oct. 1, 2015, available at
<https://www.experian.com/assets/securityupdate/securityupdate-press-release.pdf> (last
visited April 14, 2016).

1 information is then compiled and used in their credit criteria
2 when evaluating the risk level of an applicant.⁶

3 71. In addition, on October 1, 2015, T-Mobile posted a letter from its CEO
4 John J. Legere on its website regarding its reaction to the Data Breach:

5 We have been notified by Experian, a vendor that processes
6 our credit applications, that they have experienced a data
7 breach. The investigation is ongoing, but what we know right
8 now is that the hacker acquired the records of approximately
9 15 million people, including new applicants requiring a credit
10 check for service or device financing from September 1, 2013
11 through September 16, 2015. These records include
12 information such as name, address and birthdate as well as
13 encrypted fields with Social Security number and ID number
14 (such as driver's license or passport number), and additional
15 information used in T-Mobile's own credit assessment.
16 Experian has determined that this encryption may have been
17 compromised. We are working with Experian to take
18 protective steps for all of these consumers as quickly as
19 possible.

20 Obviously I am incredibly angry about this data breach and we
21 will institute a thorough review of our relationship with
22 Experian I take our customer and prospective customer
23 privacy VERY seriously. This is no small issue for us...

24 ...

25 At T-Mobile, privacy and security is of utmost importance, so
26 I will stay very close to this issue and I will do everything
27 possible to continue to earn your trust every day.⁷

28 72. T-Mobile also posted the following information on its website:

- ***Experian has taken full responsibility for the theft of data***
from its server.

⁶ <http://www.experian.com/data-breach/t-mobilefacts.html> (last visited April 14, 2016) (emphasis added).

⁷ <http://www.t-mobile.com/landing/experian-data-breach.html> (last visited April 14, 2016) (emphasis added).

- 1 • ***Experian maintains a historical record of the applicant data***
2 ***used by T-Mobile to make credit decisions.*** The data
3 provides the record of the applicant's credit application with
4 T-Mobile and is used to assist with credit decisions and
5 respond to questions from applicants about the decision on
6 their credit application. ***The data is required to be***
maintained for a minimum period of 25 months under credit
laws.
- 7 • All of our vendors are contractually obligated to abide by
8 stringent privacy and security practices, and we regularly
9 conduct reviews of vendor security practices as necessary.
10 That was no different with Experian.
- 11 • Experian determined that, although Social Security and
12 identification numbers were encrypted, the ***encryption may***
have been compromised.
- 13 • Our vendors are contractually obligated to abide by stringent
14 privacy and security practices, and ***we are extremely***
15 ***disappointed that hackers could access the Experian***
16 ***network.***⁸

17 73. On October 8, 2015 and thereafter, Experian updated its website. Most
18 notably, Experian clarified that, *in addition to T-Mobile applicants*, other customers'
19 and organizations' identifying and personal information was accessed during the breach.
20 It also admitted that it had "disclosed" the information, and that the information had
21 been "downloaded":

- 22 • Based on Experian's investigation to date, the unauthorized
23 access ... included access to a server that contained
24 identifying information for some organizations and, primarily,
25 personal information for individuals, including some current
26 customers, and also consumers who applied for T-Mobile

27
28 ⁸ See *Frequently Asked Questions About the Experian Incident*, T-MOBILE, Oct. 8, 2015,
available at <http://www.t-mobile.com/landing/experian-data-breach-faq.html> (last
visited April 14, 2016).

1 USA postpaid service or device financing, which require a
2 credit check, from Sept. 1, 2013 through Sept. 16, 2015.

- 3 • Based on our investigation to date, *some organizations had*
4 *unauthorized disclosure of identifying information* and
5 individuals, including some current customers, and also
6 consumers who applied for service or device financing from
7 Sept. 1, 2013 through Sept. 16, 2015, *had unauthorized*
8 *disclosure of their personal information*. Records containing
9 a name, address, Social Security number, date of birth,
10 identification number (typically a driver's license, military ID,
11 or passport number) and additional information used in T-
12 Mobile's own credit assessment *were downloaded*.⁹

13 74. According to the California Attorney General's February 2016 *California*
14 *Data Breach Report*, the Data Breach affected approximately 2.1 million individuals *in*
15 *California alone*.¹⁰ The extent of the impact on consumers has prompted Attorneys
16 General from several states, including at least Massachusetts, Illinois, and Connecticut,
17 to initiate a multi-state investigation into Experian's role in the Data Breach.¹¹

18 **B. Experian Promised to Protect Its Customers' PII, but Maintained**
19 **Inadequate Data Security.**

20 75. Experian is one of the major credit reporting bureaus in the United States.
21 As a credit bureau service, Experian is engaged in a number of credit-related services,
22 including "[a]ssisting organizations with evaluating the risks and rewards associated
23 with providing credit to consumers and businesses," and providing people with "online
24 access to their credit history and score." Experian also maintains information related to
25 the credit history of consumers and provides the information to credit grantors who are
26 considering a borrower's application for credit or who have extended credit to the

27 ⁹ <http://www.experian.com/data-breach/t-mobilefacts.html> (last visited April 14, 2016).

28 ¹⁰ See CALIFORNIA DEPARTMENT OF JUSTICE, *California Data Breach Report*, Feb. 16,
2016, available at <https://oag.ca.gov/breachreport2016> (last visited April 14, 2016).

¹¹ <http://www.reuters.com/article/2015/10/02/us-experian-cyberattack-investigation-idUSKCN0RW2BC20151002> (last visited April 14, 2016).

1 borrower.¹²

2 76. Prior to the Data Breach, Experian promised its customers and everyone
3 else whose PII it collects that it would reasonably protect their PII. Experian's privacy
4 policy stated, in relevant part:

5 Experian is held accountable for its information use by
6 consumer privacy expectations and by laws and industry codes
7 established by government entities and industry organizations
8 around the world.

9 Among the laws and industry self-regulatory codes with which
10 Experian complies in the United States are:

- 11 • The Fair Credit Reporting Act.
- 12 • The Gramm-Leach-Bliley Act¹³

13 77. Experian's policy further stated: "We use a variety of security systems to
14 safeguard the information we maintain and provide We comply with all laws and
15 applicable self-regulatory guidelines We comply with all contractual restrictions
16 placed on information provided to Experian."¹⁴

17 78. Plaintiffs and Class members were required to disclose their PII to
18 Experian in connection with their use of Experian's services (including credit
19 assessments for T-Mobile), and Experian compiled, maintained, and furnished Class
20 members' PII, in connection with Class members' acquisition of services, such as
21 mobile phone service. Experian was allowed to perform such services, involving such
22 sensitive information only if it adhered to the requirements of laws meant to protect the
23 privacy of such information, such as the FCRA and the Gramm-Leach-Bliley Act
24 ("GLBA"). Experian's maintenance, use, and furnishing of such PII is and was

25
26 ¹² See *Experian's Principal Business Groups*, EXPERIAN,
27 <http://www.experian.com/corporate/principal-businesses.html> (last visited April 14,
2016).

28 ¹³ <http://www.experian.com/privacy/accountability.html> (last visited April 14, 2016).

¹⁴ http://www.experian.com/privacy/information_values.html (last visited April 14,
2016).

1 intended to affect Plaintiffs and other Class members, and the harm caused by
2 disclosure of that PII in the Data Breach was entirely foreseeable to Experian.

3 79. Experian has also touted itself as an industry leader in data breach security
4 and often promotes the importance of data breach prevention. Experian annually
5 publishes both a Data Breach Response Guide¹⁵ and a Data Breach Industry Forecast.¹⁶
6 Both publications state that Experian is “a leader in helping businesses plan for and
7 mitigate consumer risk following data breach incidents,” and that Experian “offers
8 incident management, notification, call center support and reporting services while
9 serving millions of affected consumers with proven credit and identity protection
10 products.”¹⁷ The Data Breach Response Guide also emphasizes the importance of
11 taking a number of proactive measures to prevent data breaches, which Experian failed
12 to adopt to prevent the Data Breach.¹⁸

13 80. Similarly, Experian touts its expertise in its annual report. For instance, in
14 its 2015 Annual Report, Experian stated:

15 We may experience cyber attacks on us, our partners or third-
16 party contractors How do we manage the risk?

- 17 • We have a number of defensive and proactive practices across
18 the Group, based on our global security policies.
- 19 • A programme of continuous measurement and alerting helps
20 ensure that we quickly highlight areas of risk in our business
21 practices and manage them accordingly.
- 22 • Our enterprise risk management framework works to create
23 transparency across layers of management and seeks to ensure
24 we have appropriate oversight of data security, privacy and

25 ¹⁵ See Experian Data Breach Resolution, *Data Breach Response Guide* (2014-15 ed.),
26 available at <http://www.experian.com/assets/data-breach/brochures/2014-2015-data-breach-response-guide.pdf> (last visited April 14, 2016).

27 ¹⁶ See Experian Data Breach Resolution, *Experian Data Breach Industry Forecast*,
28 2015, available at <https://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf> (last visited April 14, 2016).

¹⁷ See *id.*

¹⁸ See *Data Breach Response Guide*, *supra* n.15.

protection.¹⁹

C. Experian Experienced Prior Data Breaches, but Nevertheless Failed to Implement Appropriate Security.

81. Although Experian claims to be a leader in data security and in managing data breaches once they occur, and its privacy policy promises to reasonably safeguard consumer data, Experian's own data security practices were inadequate. Experian was well aware of this fact because it had experienced multiple data breaches in recent years.

82. For example, the Privacy Rights Clearinghouse data breach compilation website (www.privacyrights.org/data-breach) reveals at least two separate breaches in 2012 in which an *"unauthorized user or users was able to access credit monitoring information after managing to pass Experian's authentication process."*²⁰

83. In October 2012, Bloomberg News reported that Experian experienced 86 data breaches through the accounts of client organizations such as banks and auto dealers.²¹

84. In 2013, Court Ventures, a court record collection service Experian acquired 10 months earlier, sold the personal information—including Social Security numbers and banking information—of millions of consumers to an unauthorized individual posing as a private investigator. This individual then resold the information to cybercriminals for nearly \$2 million. Experian failed to notice the illegal activity for nine months and only became aware of the problem when the United States Secret Service alerted the company.²² According to the United States Department of Justice, over 13,000 individuals whose information was sold were victimized by the filing of

¹⁹ Experian 2015 Annual Report (as of June 12, 2015), pp. 16-17, *available at* <http://annualreport.experianplc.com/2015/resources/pdf/Experian%20Annual%20Report%202015.pdf> (last visited April 14, 2016).

²⁰ See <https://www.privacyrights.org/node/54448> (last visited April 14, 2016); <https://www.privacyrights.org/node/54516> (last visited April 14, 2016).

²¹ *Top Credit Agencies Say Hackers Stole Celebrity Reports*, Bloomberg, Mar. 12, 2013, <http://www.bloomberg.com/news/articles/2013-03-12/equifax-transunion-say-hackers-stole-celebrity-reports> (last visited April 14, 2016).

²² <http://krebsonsecurity.com/2014/03/experian-lapse-allowed-id-theft-service-to-access-200-million-consumer-records/> (last visited April 14, 2016).

1 \$65 million in fraudulent income tax returns.²³

2 85. In December 2013, eight months after acquiring Decisioning Solutions, an
3 identity-proofing and authentication company, Experian suffered a data breach that also
4 involved T-Mobile customer data. This time, unauthorized individuals gained access to
5 a Decisioning Solutions file stored on servers owned by Experian. The file contained
6 names, Social Security numbers and driver's license numbers of T-Mobile customers.²⁴

7 86. In an interview with Bloomberg News, privacy advocate Dissent Doe
8 stated that, under the Freedom of Information Act, he had requested and received
9 information regarding more than 100 data breaches involving Experian's database.²⁵

10 87. As a result of these and additional incidents, Experian knew its information
11 security systems and practices were inadequate to prevent unauthorized users from
12 accessing information housed in its servers and networks. Despite these prior breaches
13 and known vulnerabilities, Experian's data security practices had already deteriorated
14 prior to the Data Breach.

15 88. According to Brian Krebs, a well-known cybersecurity reporter who has
16 uncovered many high-profile data breaches, several former members of Experian's
17 information security team complained about the inadequacy of Experian's data security
18 practices, including failures to fund important security projects or replace departing
19 staff:

20 Over the past week, KrebsOnSecurity has interviewed a half-
21 dozen security experts who said they recently left Experian to
22 find more rewarding and less frustrating work at other
23 corporations. Nearly all described Experian as a company
24 fixated on acquiring companies in the data broker and
analytics technology space, even as it has stymied efforts to
improve security and accountability at the Costa Mesa, Calif.

25 ²³ [http://krebsonsecurity.com/2015/07/experian-hit-with-class-action-over-id-theft-](http://krebsonsecurity.com/2015/07/experian-hit-with-class-action-over-id-theft-service/)
26 [service/](http://krebsonsecurity.com/2015/07/experian-hit-with-class-action-over-id-theft-service/) (last visited April 14, 2016).

27 ²⁴ <http://krebsonsecurity.com/2015/10/at-experian-security-attrition-amid-acquisitions/>
(last visited April 14, 2016).

28 ²⁵ *The Changes Coming to Credit Agencies Won't Stop Hackers*, Bloomberg, Mar. 9,
2015, [http://www.bloomberg.com/news/articles/2015-03-09/the-changes-coming-to-](http://www.bloomberg.com/news/articles/2015-03-09/the-changes-coming-to-credit-agencies-won-t-stop-hackers)
[credit-agencies-won-t-stop-hackers](http://www.bloomberg.com/news/articles/2015-03-09/the-changes-coming-to-credit-agencies-won-t-stop-hackers) (last visited April 14, 2016).

1 based firm.

2 Jasun Tate worked for a year until April 2014 as a chief
3 information security officer delegate and risk consultant at
4 Experian's government services and e-marketing business
5 units. Tate said he and several of his colleagues left last year
6 after repeatedly running into problems getting buy-in or
7 follow-up support for major projects to beef up security
8 around Experian's growing stable of companies handling
9 sensitive consumer and government data.

10 "What the board of directors at Experian wanted security-wise
11 and the security capabilities on the ground were two
12 completely different things," Tate said

13
14 After [the former Chief Information Officer] was lured away
15 to take the CIO job at the Bank of England, many of the major
16 in-progress projects designed to bake security into all aspects
17 of Experian's business ground to a halt, the former employees
18 said on condition of anonymity. Core members of the
19 Experian security team soon began seeking employment
20 elsewhere. A year after [the CIO's] departure, morale suffered
21 and the staff of the company's [security operations center] had
22 dwindled from nearly 30 to about a dozen.

23 . . .
24 "We had a period of time there where security was viewed in a
25 positive light, and things weren't being swept under the rug
26 for the sake of uptime" the employee said. "[The CIO] left
27 and it kind of went the opposite direction. Once the leadership
28 changed, the focus changed to controlling costs and not taking
systems down for maintenance, and investments started
disappearing from a lot of areas. We were in the middle of
putting into operation certain tools to do next-generation
detection of [cyber] threats, but we weren't able to get many
of them out into production. And that's how Experian wound
up where they are now."²⁶

89. It appears that even since the Data Breach, Experian continues to fail to

²⁶ *Id.*

1 implement the necessary measures to prevent further data breaches. In October 2015,
2 Experian was exposed for allowing public access to an internal portal. Mr. Krebs
3 published the following:

4 The [portal] also apparently allowed anyone to file support
5 tickets, potentially making it easy for clever attackers who'd
6 studied the exposed support tickets to fabricate a request for
7 access to Experian resources or accounts on the system.

8 In addition, experts I spoke with who examined the portal said
9 the support site allowed anyone to upload arbitrary file
10 attachments of virtually any file type. Those experts said such
11 file upload capabilities are notoriously easy for attackers to
12 use to inject malicious files into databases and other
13 computing environments, and that having such capability out
14 in the open without at least first requiring users to supply
15 valid username and password credentials is asking for
16 trouble.²⁷

17 **D. The Data Breach Has Exposed Plaintiffs and Other Consumers to**
18 **Fraud, Identity Theft, Financial Harm, and a Heightened, Imminent**
19 **Risk of Such Harm in the Future.**

20 90. Since identity thieves use the PII of other people to commit fraud or other
21 crimes, Plaintiffs and other consumers whose information was exposed in the Data
22 Breach are subject to an increased, concrete risk of identity theft. Javelin Strategy &
23 Research, a research-based consulting firm that specializes in fraud and security in
24 advising its clients, reported in its 2014 Identity Fraud Study that “[d]ata breaches are
25 the greatest risk factor for identity fraud.” In fact, “[i]n 2013, one in three consumers
26 who received notification of a data breach became a victim of fraud.” Javelin also
27 found increased instances of fraud other than credit card fraud, including “compromised
28 lines of credit, internet accounts (e.g., eBay, Amazon) and email payment accounts such
as PayPal.”²⁸

²⁷ *Id.*

²⁸ See <https://www.javelinstrategy.com/press-release/new-identity-fraud-victim-every-two-seconds-2013-according-latest-javelin-strategy> (last visited April 14, 2016).

1 91. The California Attorney General issued a statement reiterating that the
2 disclosed information in the Data Breach “could be used for identity theft, particularly
3 ‘new account fraud,’ or opening up new accounts in the victim’s name” and urged
4 affected consumers to place fraud alerts or security freezes on their credit records.²⁹

5 92. The exposure of Plaintiffs’ and Class members’ Social Security numbers in
6 particular poses serious problems. Criminals frequently use Social Security numbers to
7 create false bank accounts, file fraudulent tax returns, and incur credit in the victim’s
8 name. Neal O’Farrell, a security and identity theft expert for Credit Sesame calls a
9 Social Security number “your secret sauce,” that is “as good as your DNA to hackers.”³⁰
10 Even where data breach victims obtain a new Social Security number, the Social
11 Security Administration warns “that a new number probably will not solve all []
12 problems . . . and will not guarantee [] a fresh start.”³¹ In fact, “[f]or some victims of
13 identity theft, a new number actually creates new problems.” One of those new
14 problems is that a new Social Security number will have a completely blank credit
15 history, making it difficult to get credit for a few years unless it is linked to the old
16 compromised number.

17 93. As a result of the compromising of their PII, Plaintiffs and Class members
18 have suffered one or a combination of the following injuries:

- 19 • incidences of identity fraud and theft, including unauthorized bank activity,
20 fraudulent credit card purchases, and damage to their credit;
21 • money and time expended to prevent, detect, contest, and repair identity
22 theft, fraud, and/or other unauthorized uses of PII;

23
24
25 ²⁹ [https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-urges-t-](https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-urges-t-mobile-customers-place-fraud-alerts)
[mobile-customers-place-fraud-alerts](https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-urges-t-mobile-customers-place-fraud-alerts) (last visited April 14, 2016).

26 ³⁰ Tips, How to Protect Your Kids From the Anthem Data Breach,” Kiplinger (Feb. 10,
27 2015), *available at*
[http://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-](http://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html)
[from-the-anthem-data-brea.html](http://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html) (last visited April 14, 2016).

28 ³¹ Social Security Administration, Identity Theft and Your Social Security Number, pp.
7-8, *available at* <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Mar. 10,
2016)

- lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breach, including but not limited to efforts to research how to prevent, detect, contest, and recover from misuse of their PII; and
- loss of the opportunity to control how their PII is used.

94. Furthermore, Plaintiffs and Class members have suffered, and/or will face an increased risk of suffering in the future, the following injuries:

- money and time lost as a result of fraudulent access to and use of their financial accounts;
- loss of use of and access to their financial accounts and/or credit;
- impairment of their credit scores, ability to borrow, and/or ability to obtain credit;
- lowered credit scores resulting from credit inquiries following fraudulent activities;
- costs and lost time obtaining credit reports in order to monitor their credit records;
- money, including fees charged in some states, and time spent placing fraud alerts and security freezes on their credit records;
- money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;
- costs of credit monitoring that is more robust than the services being offered by Experian;
- anticipated future costs from the purchase of credit monitoring and/or identity theft protection services once the temporary services being offered by Experian expire;
- costs and lost time from dealing with administrative consequences of the Data Breach, including by identifying, disputing, and seeking reimbursement for fraudulent activity, canceling compromised financial

accounts and associated payment cards, and investigating options for credit monitoring and identity theft protection services;

- money and time expended to ameliorate the consequences of the filing of fraudulent tax returns; and
- continuing risks to their personal information, which remains subject to further harmful exposure and theft as long as Experian fails to undertake appropriate, legally required steps to protect the personal information in its possession.

95. The risks that Plaintiffs and Class members bear as a result of the Data Breach cannot be mitigated by the credit monitoring Experian has offered to affected consumers because it can only help detect, but will not prevent, the fraudulent use of Plaintiffs' and Class members' PII. Instead, Plaintiffs and Class members will need to spend time and money to protect themselves. For instance, credit reporting agencies impose fees for credit freezes in certain states. In addition, while credit reporting agencies offer consumers one free credit report per year, consumers who request more than one credit report per year from the same credit reporting agency (such as Experian) must pay a fee for the additional report. Such fees constitute out-of-pocket costs to Plaintiffs and Class members.

96. The risks borne by affected consumers are not hypothetical: Experian has admitted that Class members' personal information was disclosed and downloaded in the Data Breach, has admitted the risks of identity theft, and has encouraged consumers to vigilantly monitor their accounts. ***After the Data Breach, Class members' personal data reportedly quickly appeared for sale on the dark web.*** On October 3, 2015, an article entitled "Data Likely Stolen from Experian/T-Mobile Spotted for Sale on Dark Web" noted that Trustev, an Irish fraud-prevention company that monitors online sales of stolen data, released screen shots of listings for personal information that was likely compromised during the Data Breach. A Trustev spokesperson stated that Trustev "saw listings go up for FULLZ data that matches the same types of information that just came

1 out of the Experian hack.” FULLZ is a slang term for a package of PII, including Social
2 Security number and date of birth, among other things. The spokesperson stated that
3 once data thieves acquire stolen data, they typically unload it very quickly, and
4 therefore, it was “extremely likely” that the listings were from the Data Breach due to
5 the “type of data and timing.”⁷

6 **E. Experian Was Required to Insure the Security of Plaintiffs’ PII, and to**
7 **Investigate and Provide Timely and Adequate Notification of the Data**
8 **Breach under Federal Regulations, But Failed To Do So.**

9 97. In addition to the requirements of the Fair Credit Reporting Act, and
10 several state statutes, which are discussed below, the Gramm-Leach-Bliley Act
11 (“GLBA”) imposes upon “financial institutions” “an affirmative and continuing
12 obligation to respect the privacy of its customers and to protect the security and
13 confidentiality of those customers’ nonpublic personal information.” 15 U.S.C. § 6801.
14 To satisfy this obligation, financial institutions must satisfy certain standards relating to
15 administrative, technical, and physical safeguards:

16 (1) to *insure the security and confidentiality of customer records*
17 *and information;*

18 (2) to *protect against any anticipated threats or hazards to the*
19 *security or integrity of such records;* and

20 (3) to *protect against unauthorized access to or use of such*
21 *records* or information which could result in substantial harm
22 or inconvenience to any customer. 15 U.S.C. § 6801(b)
23 (emphasis added).

24 98. In order to satisfy their obligations under the GLBA, financial institutions
25 must “develop, implement, and maintain a comprehensive information security program
26 that is [1] written in one or more readily accessible parts and [2] contains administrative,
27

28 ⁷ <http://venturebeat.com/2015/10/03/data-likely-stolen-from-experiant-mobile-spotted-for-sale-on-dark-web-says-security-firm/> (last visited April 14, 2016).

1 technical, and physical safeguards that are appropriate to [their] size and complexity, the
2 nature and scope of [their] activities, and the sensitivity of any customer information at
3 issue.” *See* 16 C.F.R. § 314.4. “In order to develop, implement, and maintain [their]
4 information security program, [financial institutions] shall:

5 (a) Designate an employee or employees to coordinate [their]
6 information security program.

7
8 (b) ***Identify reasonably foreseeable internal and external risks***
9 ***to the security, confidentiality, and integrity of customer***
10 ***information*** that could result in the unauthorized disclosure,
11 misuse, alteration, destruction or other compromise of such
12 information, and assess the sufficiency of any safeguards in
13 place to control these risks. At a minimum, such a risk
14 assessment should include consideration of risks in each
15 relevant area of [their] operations, including:

16 (1) Employee training and management;

17 (2) Information systems, including network and software
18 design, as well as information processing, storage,
19 transmission and disposal; and

20 (3) Detecting, preventing and responding to attacks,
21 intrusions, or other systems failures.

22 (c) ***Design and implement information safeguards to control the***
23 ***risks [they] identify through risk assessment***, and regularly
24 test or otherwise monitor the effectiveness of the safeguards’
25 key controls, systems, and procedures.

26 (d) Oversee service providers, by:

27 (1) Taking reasonable steps to select and retain service
28 providers that are capable of maintaining appropriate
safeguards for the customer information at issue; and

(2) Requiring [their] service providers by contract to
implement and maintain such safeguards.

1 (e) ***Evaluate and adjust [their] information security program in***
2 ***light of the results*** of the testing and monitoring required by
3 paragraph (c) of this section; any material changes to [their]
4 operations or business arrangements; or any other
5 circumstances that [they] know or have reason to know may
6 have a material impact on [their] information security
program.”

7 *Id.*

8 99. In addition, under the Interagency Guidelines Establishing Information
9 Security Standards, 12 C.F.R. pt. 225, App. F, financial institutions have an affirmative
10 duty to “develop and implement a risk-based response program to address incidents of
11 unauthorized access to customer information in customer information systems.” *See id.*
12 “At a *minimum*, an institution’s response program should contain procedures for the
13 following:

- 14 a. the nature and scope of an incident, and identifying what
15 customer information systems and types of customer
16 information have been accessed or misused;
- 17 b. Notifying its primary Federal regulator as soon as possible
18 when the institution becomes aware of an incident involving
19 unauthorized access to or use of sensitive customer
20 information, as defined below;
- 21 c. Consistent with the Agencies’ Suspicious Activity Report
22 (“SAR”) regulations, notifying appropriate law enforcement
23 authorities, in addition to filing a timely SAR in situations
24 involving Federal criminal violations requiring immediate
attention, such as when a reportable violation is ongoing;
- 25 d. Taking appropriate steps to contain and control the incident to
26 prevent further unauthorized access to or use of customer
27 information, for example, by monitoring, freezing, or closing
28 affected accounts, while preserving records and other
evidence; and

1 e. Notifying customers when warranted.

2 *Id.* (emphasis added).

3 100. Further, “[w]hen a financial institution becomes aware of an incident of
4 unauthorized access to sensitive customer information, the institution should conduct a
5 reasonable investigation to promptly determine the likelihood that the information has
6 been or will be misused. If the institution determines that misuse of its information
7 about a customer has occurred or is reasonably possible, it should notify the affected
8 customer as soon as possible.” *See id.*

9 101. Credit bureaus are “financial institutions” for purposes of the GLBA, and
10 are therefore subject to its provisions. *See TranUnion LLC v. F.T.C.*, 295 F.3d 42, 48
11 (D.C. Cir. 2002). Under Regulation Y promulgated by the Federal Reserve Board, *Bank*
12 *Holding Companies and Change in Bank Control*, “credit bureau services”³² are “so
13 closely related to banking or managing or controlling banks as to be a proper incident
14 thereto.” Since Experian is a credit bureau and performs credit bureau services, it
15 qualifies as a financial institution for purposes of the GLBA.

16 102. “Nonpublic personal information,” includes PII (such as the PII
17 compromised during the Data Breach) for purposes of the GLBA. Likewise, “sensitive
18 customer information” includes PII for purposes of the Interagency Guidelines
19 Establishing Information Security Standards.

20 103. Upon information and belief, Experian failed to “develop, implement, and
21 maintain a comprehensive information security program” with “administrative,
22 technical, and physical safeguards” that were “appropriate to [its] size and complexity,
23 the nature and scope of [its] activities, and the sensitivity of any customer information at
24 issue.” This includes, but is not limited to, Experian’s failure to (a) implement and
25 maintain adequate data security practices to safeguard Class members’ PII; (b) failing to
26 detect the Data Breach in a timely manner; and (c) failing to disclose that its data

27 ³² Credit bureau services include “[m]aintaining information related to the credit history
28 of consumers and providing the information to a credit grantor who is considering a
borrower’s application for credit or who has extended credit to the borrower.” *See* 12
C.F.R. § 225.28.

1 security practices were inadequate to safeguard Class members' PII.

2 104. Upon information and belief, Experian also failed to "develop and
3 implement a risk-based response program to address incidents of unauthorized access to
4 customer information in customer information systems" as mandated by the GLBA.
5 This includes, but is not limited to, Experian's failure to notify appropriate regulatory
6 agencies, law enforcement, and the affected individuals themselves of the Data Breach
7 in a timely and adequate manner.

8 105. Upon information and belief, Experian also failed to notify affected
9 customers as soon as possible after it became aware of unauthorized access to sensitive
10 customer information.

11 CLASS ACTION ALLEGATIONS

12 106. Plaintiffs bring all claims as class claims under Federal Rule of Civil
13 Procedure 23(b)(1), (b)(2), (b)(3), and (c)(4).

14 A. Nationwide Class

15 107. Plaintiffs bring their FCRA, negligence, and negligence per se claims
16 (Counts I-IV) on behalf of a proposed nationwide class ("Nationwide Class"), defined
17 as follows:

18 *All natural persons and entities in the United States whose*
19 *personally identifiable information was acquired by unauthorized*
20 *persons in the data breach announced by Experian in October 2015.*

21 B. Statewide Subclasses

22 108. Plaintiffs bring their state consumer protection statute and/or data breach
23 notification claims (Counts 5 through 48) on behalf of separate statewide subclasses for
24 each of the following states:

- 25 a. Alabama
- 26 b. Arizona
- 27 c. California
- 28 d. Colorado

- e. Delaware
- f. Florida
- g. Georgia
- h. Hawaii
- i. Illinois
- j. Indiana
- k. Kentucky
- l. Massachusetts
- m. Michigan
- n. Minnesota
- o. Missouri
- p. Nevada
- q. New Jersey
- r. New Mexico
- s. New York
- t. North Carolina
- u. Ohio
- v. Oregon
- w. Pennsylvania
- x. South Carolina
- y. Tennessee
- z. Texas
- aa. Virginia
- bb. Washington

Each proposed statewide subclass (“Statewide Subclass”) is defined as follows:

1 *All natural persons and entities in [STATE] whose personally*
2 *identifiable information was acquired by unauthorized persons in*
3 *the data breach announced by Experian in October 2015.*

4 109. Plaintiffs also bring their negligence and negligence per se claims (counts
5 III and IV) separately on behalf of each of the Statewide Subclasses, in the alternative to
6 bringing those claims on behalf of the Nationwide Class.

7 110. Except where otherwise noted, “Class members” shall refer to members of
8 the Nationwide Class and each of the Statewide Subclasses, collectively.

9 111. Excluded from the Nationwide Class and the Statewide Subclasses are
10 Defendants and their current employees, as well as the Court and its personnel presiding
11 over this action.

12 112. The Nationwide and Statewide Subclasses meet the requirements of
13 Federal Rules of Civil Procedure 23(a) and 23(b)(1), (b)(2), and (b)(3) for all of the
14 reasons set forth in Paragraphs 39-47:

15 113. **Numerosity:** The Nationwide and Statewide Subclasses are so numerous
16 that joinder of all members is impracticable. According to Experian, the Nationwide
17 Class includes approximately 15 million individuals whose PII was acquired during the
18 Data Breach. On information and belief, Plaintiffs allege that there are also thousands to
19 millions of individuals in each Statewide Subclass. The parties will be able to identify
20 each member of the Nationwide Class and Statewide Subclasses after Defendants’
21 document production and/or related discovery.

22 114. **Commonality:** There are numerous questions of law and fact common to
23 Plaintiffs and the Nationwide Class and Statewide Subclasses, including but not limited
24 to the following:

- 25 • whether Defendants engaged in the wrongful conduct alleged herein;
- 26 • whether Defendants owed a duty to Plaintiffs and Class members to
- 27 adequately protect their PII;
- 28

- whether Defendants breached their duties to protect the personal information of Plaintiffs and Class member;
- whether Defendants knew or should have known that their data security systems and processes were vulnerable to attack;
- whether Plaintiffs and Class member suffered legally cognizable damages as a result of Defendants' conduct, including increased risk of identity theft and loss of value of PII;
- whether Defendants violated the FCRA; and
- whether Plaintiffs and Class members are entitled to equitable relief including injunctive relief.

115. **Typicality:** All Plaintiffs' claims are typical of the claims of the Nationwide Class, and each Plaintiff's claims are typical of the claims of the Statewide Subclass in which state the respective Plaintiff resides. Each of the Plaintiffs, like all proposed Class members, had their PII compromised in the Data Breach.

116. **Adequacy:** Plaintiffs will fairly and adequately protect the interests of the Nationwide Class and Statewide Subclasses. Plaintiffs have no interests that are adverse to, or in conflict with, the Class members. There are no claims or defenses that are unique to Plaintiffs. Likewise, Plaintiffs have retained counsel experienced in class action and complex litigation, including data breach litigation, that have sufficient resources to prosecute this action vigorously.

117. **Predominance:** The proposed action meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because questions of law and fact common to the Nationwide Class and Statewide Subclasses predominate over any questions which may affect only individual Class members in any of the proposed classes, including those listed in paragraph 114, *supra*.

118. **Superiority:** The proposed action also meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of

1 common questions is superior to multiple individual actions or piecemeal litigation,
2 avoids inconsistent decisions, presents far fewer management difficulties, conserves
3 judicial resources and the parties' resources, and protects the rights of each Class
4 member.

5 119. Absent a class action, the majority of Class members would find the cost of
6 litigating their claims prohibitively high and would have no effective remedy.

7 120. **Risks of Prosecuting Separate Actions:** Plaintiffs' claims also meet the
8 requirements of Federal Rule of Civil Procedure 23(b)(1) because prosecution of
9 separate actions by individual Class members would create a risk of inconsistent or
10 varying adjudications that would establish incompatible standards for Experian.
11 Experian continues to maintain the PII of the Class members and other individuals, and
12 varying adjudications could establish incompatible standards with respect to:
13 Defendants' duty to protect individuals' PII; whether Defendants' ongoing conduct
14 violates the FCRA and other claims alleged herein; and whether the injuries suffered by
15 Class members are legally cognizable, among others. Prosecution of separate actions by
16 individual Class members would also create a risk of individual adjudications that
17 would be dispositive of the interests of other Class members not parties to the individual
18 adjudications, or substantially impair or impede the ability of Class members to protect
19 their interests.

20 121. **Injunctive Relief:** In addition, Defendants have acted and/or refused to act
21 on grounds that apply generally to the Nationwide Class and Statewide Subclasses,
22 making injunctive and/or declaratory relief appropriate with respect to the classes under
23 Federal Rule of Civil Procedure 23(b)(2). Defendants continue to (1) maintain the PII
24 of Class members, (2) fail to adequately protect their PII, and (3) violate their rights
25 under the FCRA and other claims alleged herein.

26 122. **Certification of Particular Issues:** In the alternative, the Nationwide
27 Class and Statewide Subclasses may be maintained as class actions with respect to
28 particular issues, in accordance with Fed. R. Civ. P. 23(c)(4).

CAUSES OF ACTION

COUNT 1

WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT

(On Behalf of the Nationwide Class)

123. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

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

125. Under the FCRA, a “consumer reporting agency” is defined as “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” 15 U.S.C. § 1681a(f).

126. Experian is a consumer reporting agency under the FCRA because, for monetary fees, it regularly engages 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.

127. As a consumer reporting agency, the FCRA requires Experian 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).

128. Under the FCRA, a “consumer report” is defined as “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 . . . to be used primarily for personal, family, or household purposes; . . . or (C) any other purpose authorized under section 1681b of this title.” 15 U.S.C. § 1681a(d)(1).

1 129. The compromised data was a consumer report under the FCRA because it
2 was a communication of information bearing on Class members' credit worthiness,
3 credit standing, credit capacity, character, general reputation, personal characteristics, or
4 mode of living used, or expected to be used or collected in whole or in part, for the
5 purpose of serving as a factor in establishing the Class members' eligibility for credit.

6 130. As a consumer reporting agency, Experian may only furnish a consumer
7 report under the limited circumstances set forth in 15 U.S.C. § 1681b, "and no other."
8 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b permit
9 credit reporting agencies to furnish consumer reports to unauthorized or unknown
10 entities, or computer hackers such as those who accessed the Nationwide Class
11 members' PII. Experian violated § 1681b by furnishing consumer reports to
12 unauthorized or unknown entities or computer hackers, as detailed above.

13 131. Experian furnished the Nationwide Class members' consumer reports by
14 disclosing their consumer reports to unauthorized entities and computer hackers;
15 allowing unauthorized entities and computer hackers to access their consumer reports;
16 knowingly and/or recklessly failing to take security measures that would prevent
17 unauthorized entities or computer hackers from accessing their consumer reports; and/or
18 failing to take reasonable security measures that would prevent unauthorized entities or
19 computer hackers from accessing their consumer reports.

20 132. The Federal Trade Commission ("FTC") has pursued enforcement actions
21 against consumer reporting agencies under the FCRA for failing to "take adequate
22 measures to fulfill their obligations to protect information contained in consumer
23 reports, as required by the" FCRA, in connection with data breaches.³³

24 133. Experian willfully and/or recklessly violated § 1681b and § 1681e(a) by
25 providing impermissible access to consumer reports and by failing to maintain
26 reasonable procedures designed to limit the furnishing of consumer reports to the

27
28 ³³ Statement of Commissioner Brill (Federal Trade Commission 2011), *available at*
<<https://www.ftc.gov/sites/default/files/documents/cases/2011/08/110819settlementonstatements.pdf>> (last visited April 14, 2016).

1 purposes outlined under section 1681b of the FCRA. The willful and reckless nature of
2 Experian's violations is supported by, among other things, former employees'
3 admissions that Experian's data security practices have deteriorated in recent years, and
4 Experian's numerous other data breaches in the past. Further, Experian touts itself as an
5 industry leader in breach prevention; thus, Experian was well aware of the importance
6 of the measures organizations should take to prevent data breaches, and willingly failed
7 to take them.

8 134. Experian also acted willfully and recklessly because it knew or should have
9 known about its legal obligations regarding data security and data breaches under the
10 FCRA. These obligations are well established in the plain language of the FCRA and in
11 the promulgations of the Federal Trade Commission. *See, e.g.*, 55 Fed. Reg. 18804
12 (May 4, 1990), 1990 Commentary On The Fair Credit Reporting Act. 16 C.F.R. Part
13 600, Appendix To Part 600, Sec. 607 2E. Experian obtained or had available these and
14 other substantial written materials that apprised them of their duties under the FCRA.
15 Any reasonable consumer reporting agency knows or should know about these
16 requirements. Despite knowing of these legal obligations, Experian acted consciously in
17 breaching known duties regarding data security and data breaches and depriving
18 Plaintiffs and other members of the classes of their rights under the FCRA.

19 135. Experian's willful and/or reckless conduct provided a means for
20 unauthorized intruders to obtain and misuse Plaintiffs' and Nationwide Class members'
21 personal information for no permissible purposes under the FCRA.

22 136. Plaintiffs and the Nationwide Class members have been damaged by
23 Experian's willful or reckless failure to comply with the FCRA. Therefore, Plaintiffs
24 and each of the Nationwide Class members are entitled to recover "any actual damages
25 sustained by the consumer . . . or damages of not less than \$100 and not more than
26 \$1,000." 15 U.S.C. § 1681n(a)(1)(A).

27 137. Plaintiffs and the Nationwide Class members are also entitled to punitive
28 damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a)(2),

(3).

COUNT 2

NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT

(On Behalf of the Nationwide Class)

138. Plaintiffs incorporate by reference all paragraphs above as if fully set forth here.

139. Experian was negligent in failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. Experian's negligent failure to maintain reasonable procedures is supported by, among other things, former employees' admissions that Experian's data security practices have deteriorated in recent years, and Experian's numerous other data breaches in the past. Further, as an enterprise claiming to be an industry leader in data breach prevention, Experian was well aware of the importance of the measures organizations should take to prevent data breaches, yet failed to take them.

140. Experian's negligent conduct provided a means for unauthorized intruders to obtain Plaintiffs' and the Nationwide Class members' PII and consumer reports for no permissible purposes under the FCRA.

141. Plaintiffs and the Nationwide Class member have been damaged by Experian's negligent failure to comply with the FCRA. Therefore, Plaintiffs and each of the Nationwide Class member are entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. § 1681o(a)(1).

142. Plaintiffs and the Nationwide Class member are also entitled to recover their costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. § 1681o(a)(2).

COUNT 3

NEGLIGENCE

(On Behalf of the Nationwide Class and Each of the Statewide Subclasses)

143. Plaintiffs incorporate by reference all paragraphs above as if fully set forth here.

1 144. Experian owed a duty to Plaintiffs and Class members, arising from the
2 sensitivity of the information and the foreseeability of its data safety shortcomings
3 resulting in an intrusion, to exercise reasonable care in safeguarding their sensitive
4 personal information. This duty included, among other things, designing, maintaining,
5 monitoring, and testing Experian's security systems, protocols, and practices to ensure
6 that Class members' information was adequately secured from unauthorized access.

7 145. Experian's privacy policy acknowledged Experian's duty to adequately
8 protect Class members' PII.

9 146. Experian owed a duty to Class members to implement intrusion detection
10 processes that would detect a data breach in a timely manner.

11 147. Experian also had a duty to delete any PII that was no longer needed to
12 serve client needs.

13 148. Experian owed a duty to disclose the material fact that its data security
14 practices were inadequate to safeguard Class members' PII.

15 149. Experian also had independent duties under Plaintiffs' and Class members'
16 state laws that required Experian to reasonably safeguard Plaintiffs' and Class members'
17 PII and promptly notify them about the Data Breach.

18 150. Experian had a special relationship with Plaintiffs and Class members from
19 being entrusted with their PII, which provided an independent duty of care. Plaintiffs'
20 and other Class members' willingness to entrust Experian with their PII was predicated
21 on the understanding that Experian would take adequate security precautions.
22 Moreover, Experian had the ability to protect its systems and the PII it stored on them
23 from attack.

24 151. Experian's role to utilize and purportedly safeguard Plaintiffs' and Class
25 members' PII presents unique circumstances requiring a reallocation of risk.

26 152. Experian breached its duties by, among other things: (a) failing to
27 implement and maintain adequate data security practices to safeguard Class members'
28 PII; (b) failing to detect the Data Breach in a timely manner; (c) failing to disclose that

Defendants' data security practices were inadequate to safeguard Class members' PII; and (d) failing to provided adequate and timely notice of the Data Breach.

153. But for Experian's breach of its duties, Class members' PII would not have been accessed by unauthorized individuals.

154. Plaintiffs and Class members were foreseeable victims of Experian's inadequate data security practices. Experian knew or should have known that a breach of its data security systems would cause damages to Class members.

155. Experian's negligent conduct provided a means for unauthorized intruders to obtain Plaintiffs' and the Nationwide Class members' PII and consumer reports for no permissible purposes under the FCRA.

156. As a result of Experian's willful failure to prevent the Data Breach, Plaintiffs and Class members suffered injury, which includes but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class members must monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Class members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs' and Class members' PII has also diminished the value of the PII.

157. The damages to Plaintiffs and the Class members were a proximate, reasonably foreseeable result of Experian's breaches of its duties.

158. Therefore, Plaintiffs and Class members are entitled to damages in an amount to be proven at trial.

COUNT 4

NEGLIGENCE PER SE

(On behalf of the Nationwide Class and Each of the Statewide Subclasses)

159. Plaintiffs incorporate by reference all paragraphs above as if fully set forth here.

1 160. Under the FCRA, 15 U.S.C. §§ 1681e, Experian is required to “maintain
2 reasonable procedures designed to . . . limit the furnishing of consumer reports to the
3 purposes listed under section 1681b of this title.” 15 U.S.C. § 1681e(a).

4 161. Defendants failed to maintain reasonable procedures designed to limit the
5 furnishing of consumer reports to the purposes outlined under section 1681b of the
6 FCRA.

7 162. Plaintiffs and Class members were foreseeable victims of Experian’s
8 violation of the FCRA. Experian knew or should have known that a breach of its data
9 security systems would cause damages to Class members.

10 163. As alleged above, Experian was required under the Gramm-Leach-Bliley
11 Act (“GLBA”) to satisfy certain standards relating to administrative, technical, and
12 physical safeguards:

13 (1) to *insure the security and confidentiality of customer records and*
14 *information;*

15 (2) to *protect against any anticipated threats or hazards to the security or*
16 *integrity of such records;* and

17 (3) to *protect against unauthorized access to or use of such records* or
18 information which could result in substantial harm or inconvenience to any
19 customer.

20 15 U.S.C. § 6801(b) (emphasis added).

21 164. In order to satisfy their obligations under the GLBA, Experian was also
22 required to “develop, implement, and maintain a comprehensive information security
23 program that is [1] written in one or more readily accessible parts and [2] contains
24 administrative, technical, and physical safeguards that are appropriate to [its] size and
25 complexity, the nature and scope of [its] activities, and the sensitivity of any customer
26 information at issue.” *See* 16 C.F.R. § 314.4.

27 165. In addition, under the Interagency Guidelines Establishing Information
28 Security Standards, 12 C.F.R. pt. 225, App. F., Experian had an affirmative duty to

1 “develop and implement a risk-based response program to address incidents of
2 unauthorized access to customer information in customer information systems.” *See id.*

3 166. Further, when Experian became aware of “unauthorized access to sensitive
4 customer information,” it should have “conduct[ed] a reasonable investigation to
5 promptly determine the likelihood that the information has been or will be misused” and
6 “notif[ied] the affected customer[s] as soon as possible.” *See id.*

7 167. Experian violated by GLBA by failing to “develop, implement, and
8 maintain a comprehensive information security program” with “administrative,
9 technical, and physical safeguards” that were “appropriate to [its] size and complexity,
10 the nature and scope of [its] activities, and the sensitivity of any customer information at
11 issue.” This includes, but is not limited to, Experian’s failure to implement and maintain
12 adequate data security practices to safeguard Class members’ PII; (b) failing to detect
13 the Data Breach in a timely manner; and (c) failing to disclose that Defendants’ data
14 security practices were inadequate to safeguard Class members’ PII.

15 168. Experian also violated the GLBA by failing to “develop and implement a
16 risk-based response program to address incidents of unauthorized access to customer
17 information in customer information systems.” This includes, but is not limited to,
18 Experian’s failure to notify appropriate regulatory agencies, law enforcement, and the
19 affected individuals themselves of the Data Breach in a timely and adequate manner.

20 169. Experian also violated by the GLBA by failing to notify affected customers
21 as soon as possible after it became aware of unauthorized access to sensitive customer
22 information.

23 170. Plaintiffs and Class members were foreseeable victims of Experian’s
24 violation of the GLBA. Experian knew or should have known that its failure to take
25 reasonable measures to prevent a breach of its data security systems, and failure to
26 timely and adequately notify the appropriate regulatory authorities, law enforcement,
27 and Class members themselves would cause damages to Class members.

28 171. Defendants’ failure to comply with the applicable laws and regulations,

1 including the FCRA and the GLBA, constitutes negligence *per se*.

2 172. But for Experian's violation of the applicable laws and regulations, Class
3 members' PII would not have been accessed by unauthorized individuals.

4 173. As a result of Experian's failure to comply with applicable laws and
5 regulations, Plaintiffs and Class members suffered injury, which includes but is not
6 limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial
7 harm. Plaintiffs and Class members must monitor their financial accounts and credit
8 histories more closely and frequently to guard against identity theft. Class members
9 also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs
10 for obtaining credit reports, credit freezes, credit monitoring services, and other
11 protective measures to deter or detect identity theft. The unauthorized acquisition of
12 Plaintiffs and Class members' PII has also diminished the value of the PII.

13 174. The damages to Plaintiffs and the Class members were a proximate,
14 reasonably foreseeable result of Experian's breaches of it's the applicable laws and
15 regulations.

16 175. Therefore, Plaintiffs and Class members are entitled to damages in an
17 amount to be proven at trial.

18 **i. Alabama**

19 **COUNT 5**

20 **VIOLATION OF THE ALABAMA DECEPTIVE TRADE PRACTICES ACT**

21 **Ala. Code § 8-19-1, et seq.**

22 **(On Behalf of the Alabama Subclass)**

23 176. Plaintiffs incorporate by reference all paragraphs above as if fully set forth
24 herein.

25 177. The Alabama Deceptive Trade Practices Act ("Alabama DTPA") declares
26 several deceptive acts or practices in the conduct of any trade or commerce to be
27 unlawful, including: "(5) [r]epresenting that goods or services have sponsorship,
28 approval, characteristics, ingredients, uses, benefits, or qualities that they do not have,"

1 “(7) [r]epresenting that goods or services are of a particular standard, quality, or grade,
2 or that goods are of a particular style or model, if they are of another,” and “(27)
3 [e]ngaging in any other unconscionable, false, misleading, or deceptive act or practice in
4 the conduct of trade or commerce.” Ala. Code § 8-19-5.

5 178. Experian, while operating in Alabama, engaged in deceptive acts and
6 practices in the conduct of trade and commerce, in violation of Ala. Code § 8-19-5(5),
7 (7), and (27). This includes but is not limited to the following:

8 a. Experian failed to enact adequate privacy and security measures to
9 protect the Alabama Subclass members’ PII from unauthorized disclosure, release, data
10 breaches, and theft, which was a direct and proximate cause of the Data Breach;

11 b. Experian failed to take proper action following known security risks
12 and prior cybersecurity incidents, which was a direct and proximate cause of the Data
13 Breach;

14 c. Experian knowingly and fraudulently misrepresented that it would
15 maintain adequate data privacy and security practices and procedures to safeguard the
16 Alabama Subclass members’ PII from unauthorized disclosure, release, data breaches,
17 and theft;

18 d. Experian omitted, suppressed, and concealed the material fact of the
19 inadequacy of its privacy and security protections for the Alabama Subclass members’
20 PII;

21 e. Experian knowingly and fraudulently misrepresented that it would
22 comply with the requirements of relevant federal and state laws pertaining to the privacy
23 and security of the Alabama Subclass members’ PII, including but not limited to duties
24 imposed by the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801 *et seq.*;

25 f. Experian failed to maintain the privacy and security of the Alabama
26 Subclass members’ PII, in violation of duties imposed by applicable federal and state
27 laws, including but not limited to those mentioned in the aforementioned paragraph,
28 directly and proximately causing the Data Breach.

1 179. As a direct and proximate result of Defendants' unlawful practices,
2 Alabama Subclass members suffered injury and/or damages, including but not limited to
3 time and expenses related to monitoring their financial accounts for fraudulent activity,
4 an increased, imminent risk of fraud and identity theft, and loss of value of their PII.

5 180. The above unlawful and deceptive acts and practices and acts by Experian
6 were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial
7 injury to the Alabama Subclass members that they could not reasonably avoid; this
8 substantial injury outweighed any benefits to consumers or to competition.

9 181. Experian knew or should have known that its computer systems and data
10 security practices were inadequate to safeguard Alabama Subclass members' PII and
11 that risk of a data breach or theft was highly likely. Defendants' actions in engaging in
12 the above-named unfair practices and deceptive acts were negligent, knowing and
13 willful, and/or wanton and reckless with respect to the rights of members of the
14 Alabama Subclass members.

15 182. A written pre-suit demand under Ala. Code § 8-19-10(e) is unnecessary
16 and unwarranted because Experian has long had notice of Plaintiffs' allegations, claims
17 and demands, including from the filing of numerous underlying actions against it arising
18 from the Data Breach, the first of which were filed on or about October 2, 2015.
19 Further, Experian is the party with the most knowledge of the underlying facts giving
20 rise to Plaintiffs' allegations, so that any pre-suit notice would not put Experian in a
21 better position to evaluate those claims.

22 183. Pursuant to Ala. Code § 8-19-10, Plaintiffs and the Alabama Subclass seek
23 monetary relief against Defendants measured as the greater of (a) actual damages in an
24 amount to be determined at trial and (b) statutory damages in the amount of \$100 for
25 each Plaintiff and each Alabama Subclass member.

26 184. Plaintiffs also seek an order enjoining Defendants' unfair, unlawful, and/or
27 deceptive practices, attorneys' fees, and any other just and proper relief available under
28 the Alabama Deceptive Trade Practices Act, Ala. Code § 8-19-1, *et seq.*

1 **ii. Arizona**

2 **COUNT 6**

3 **VIOLATION OF THE ARIZONA CONSUMER FRAUD ACT**

4 **Ariz. Rev. Stat. § 44-1521, *et seq.***

5 **(On Behalf of the Arizona Subclass)**

6 185. Plaintiffs incorporate by reference all paragraphs above as if fully set forth
7 herein.

8 186. Experian, while operating in Arizona, used and employed deception,
9 deceptive and unfair acts and practices, fraud, misrepresentation, and the concealment,
10 suppression, and omission of material facts with the intent that others rely on such
11 concealment, suppression and omission, in connection with the sale and advertisement
12 of services, in violation of Ariz. Rev. Stat.. § 44- 1522(A). This includes but is not
13 limited the following:

14 a. Experian failed to enact adequate privacy and security measures to
15 protect the Arizona Subclass members' PII from unauthorized disclosure, release, data
16 breaches, and theft, which was a direct and proximate cause of the Data Breach;

17 b. Experian failed to take proper action following known security risks
18 and prior cybersecurity incidents, which was a direct and proximate cause of the Data
19 Breach;

20 c. Experian knowingly and fraudulently misrepresented that they would
21 maintain adequate data privacy and security practices and procedures to safeguard
22 Arizona Subclass members' PII from unauthorized disclosure, release, data breaches,
23 and theft;

24 d. Experian knowingly omitted, suppressed, and concealed the
25 inadequacy of its privacy and security protections for the Arizona Subclass members'
26 PII;

27 e. Experian knowingly and fraudulently misrepresented that they would
28 comply with the requirements of relevant federal and state laws pertaining to the privacy

1 and security of Arizona Subclass members' PII, including but not limited to duties
2 imposed by the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801 *et seq.*;

3 f. Experian failed to maintain the privacy and security of Arizona
4 Subclass members' PII, in violation of duties imposed by applicable federal and state
5 laws, including but not limited to those mentioned in the aforementioned paragraph,
6 which was a direct and proximate cause of the Data Breach; and

7 g. Experian failed to disclose the Data Breach to the Arizona Subclass
8 members in a timely and accurate manner, in violation of Ariz. Rev. Stat. § 44-7501, *et*
9 *seq.*

10 187. As a direct and proximate result of Experian's practices, the Arizona
11 Subclass members suffered the injury and/or damages described herein, including but
12 not limited to time and expenses related to monitoring their financial accounts for
13 fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of
14 value of their PII.

15 188. The above unfair and deceptive practices and acts by Experian were
16 immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury
17 to the Arizona Subclass members that they could not reasonably avoid; this substantial
18 injury outweighed any benefits to consumers or to competition.

19 189. Experian knew or should have known that their computer systems and data
20 security practices were inadequate to safeguard the Arizona Subclass members' PII and
21 that the risk of a data breach or theft was highly likely. Experian's actions were
22 negligent, knowing and willful, and/or wanton and reckless with respect to the rights of
23 the Arizona Subclass members.

24 190. Plaintiffs and the Arizona Subclass seek monetary relief against Experian
25 in an amount to be determined at trial.

26 191. Plaintiffs also seek an order enjoining Defendants' unfair, unlawful, and/or
27 deceptive practices, attorneys' fees, and any other just and proper relief available under
28 the Arizona Consumer Fraud Act, Arizona Rev. Stat. § 44- 1522, *et seq.*

1 **iii. California**

2 **COUNT 7**

3 **VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW**

4 **Cal. Bus. & Prof. Code § 17200, *et seq.***

5 **(On Behalf of the Nationwide Class or, in the Alternative, the California Subclass)**

6 192. Plaintiffs incorporate by reference all paragraphs above as if fully set forth
7 herein.

8 193. California Business & Professions Code § 17200 prohibits any “unlawful,
9 unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading
10 advertising.” For the reasons discussed above, Experian violated (and continues to
11 violate) California’s Unfair Competition Law, California Business & Professions Code
12 § 17200 *et seq.*, by engaging in the above-described unlawful, unfair, fraudulent,
13 deceptive, untrue, and misleading acts and practices.

14 194. Experian’s unfair and fraudulent acts and practices include but are not
15 limited to the following:

16 a. Experian failed to enact adequate privacy and security measures, in
17 California, to protect the Class members’ PII from unauthorized disclosure, release, data
18 breaches, and theft, in violation of industry standards and best practices, which was a
19 direct and proximate cause of the Data Breach;

20 b. Experian failed to take proper action, in California, following known
21 security risks and prior cybersecurity incidents, which was a direct and proximate cause
22 of the Data Breach;

23 c. Experian knowingly and fraudulently misrepresented, in California,
24 that they would maintain adequate data privacy and security practices and procedures to
25 safeguard Class members’ PII from unauthorized disclosure, release, data breaches, and
26 theft;

1 d. Experian knowingly and fraudulently misrepresented that it did and
2 would comply with the requirements of relevant federal and state laws pertaining to the
3 privacy and security of Class members' PII;

4 e. Experian knowingly omitted, suppressed, and concealed the
5 inadequacy of its privacy and security protections for Class members' PII;

6 f. Experian failed to maintain reasonable security, in violation of Cal.
7 Civ. Code § 1798.81.5; and

8 g. Experian failed to disclose the Data Breach to Class members in a
9 timely and accurate manner, in violation of the duties imposed by Cal. Civ. Code
10 § 1798.82 *et seq.*

11 195. Experian's acts and practices also constitute "unfair" business acts and
12 practices, in that the harm caused by Experian's wrongful conduct outweighs any utility
13 of such conduct, and such conduct (i) offends public policy, (ii) is immoral,
14 unscrupulous, unethical, oppressive, deceitful and offensive, and/or (iii) has caused and
15 will continue to cause substantial injury to consumers such as Plaintiffs and the Class.

16 196. Experian's acts and practices also constitute "unlawful" business acts and
17 practices by virtue of their violation of the FCRA, 15 U.S.C. §§ 1681e (as described
18 fully above), the GLBA, 15 U.S.C. § 6801 *et seq.* (as described fully above),
19 California's fraud and deceit statutes, Cal. Civ. Code §§ 1572, 1573, 1709, 1711; Cal.
20 Bus. & Prof. Code §§ 17200, *et seq.*, 17500, *et seq.*, the California Customer Records'
21 Act, Cal. Civ. Code §§ 1798.80, *et seq.* (as described fully below), and California
22 common law.

23 197. There were reasonably available alternatives to further Experian's
24 legitimate business interests, including using best practices to protect Class members'
25 PII, other than Experian's wrongful conduct described herein.

26 198. As a direct and/or proximate result of Experian's unfair practices,
27 Plaintiffs, the Nationwide Class, and the California Subclass have suffered injury in fact
28 in connection with the Data Breach, including but not limited to time and expenses

1 related to monitoring their financial accounts for fraudulent activity, an increased,
2 imminent risk of fraud and identity theft, and loss of value of their PII. As a result,
3 Plaintiffs and other Class members are entitled to compensation, restitution,
4 disgorgement, and/or other equitable relief. Cal. Bus. & Prof. Code § 17203.

5 199. Experian knew or should have known that its data security practices and
6 infrastructure were inadequate to safeguard Class members' PII, and that the risk of a
7 data breach or theft was highly likely. Defendants' actions in engaging in the above
8 named unfair practices and deceptive acts were negligent, knowing and willful, and/or
9 wanton and reckless with respect to Class members' rights.

10 200. On information and belief, Experian's unlawful and unfair business
11 practices, except as otherwise indicated herein, continue to this day and are ongoing.

12 201. Plaintiffs and other Class members also are entitled to injunctive relief,
13 under California Business and Professions Code §§ 17203, 17204, to stop Experian's
14 wrongful acts and to require Experian to maintain adequate security measures to protect
15 the personal and financial information in its possession.

16 202. Under Business and Professions Code § 17200 *et seq.*, Plaintiffs seek
17 restitution of money or property that the Defendants may have acquired by means of
18 Defendants' deceptive, unlawful, and unfair business practices (to be proven at trial),
19 restitutionary disgorgement of all profits accruing to Defendants because of their
20 unlawful and unfair business practices (to be proven at trial), declaratory relief, and
21 attorney's fees and costs (allowed by Cal. Code Civil Pro. §1021.5).

22 **COUNT 8**

23 **VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT**

24 **Cal. Civ. Code § 1798.80, *et seq.***

25 **(On Behalf of the California Subclass)**

26 203. Plaintiffs incorporate by reference all paragraphs above as if fully set forth
27 herein.
28

1 204. “[T]o ensure that personal information about California residents is
2 protected,” Civil Code § 1798.81.5 requires any “business that owns, licenses, or
3 maintains personal information about a California resident [to] implement and maintain
4 reasonable security procedures and practices appropriate to the nature of the
5 information, to protect the personal information from unauthorized access, destruction,
6 use, modification, or disclosure.”

7 205. Experian owns, maintains, and licenses personal information, within the
8 meaning of § 1798.81.5, about Plaintiffs and the California Subclass.

9 206. Experian violated Civil Code § 1798.81.5 by failing to implement
10 reasonable measures to protect Class members’ PII.

11 207. As a direct and proximate result of Defendants’ violations of section
12 1798.81.5 of the California Civil Code, the Data Breach described above occurred.

13 208. In addition, California Civil Code § 1798.82(a) provides that “[a] person or
14 business that conducts business in California, and that owns or licenses computerized
15 data that includes personal information, shall disclose a breach of the security of the
16 system following discovery or notification of the breach in the security of the data to a
17 resident of California whose unencrypted personal information was, or is reasonably
18 believed to have been, acquired by an unauthorized person. The disclosure shall be
19 made in the most expedient time possible and without unreasonable delay”

20 209. Section 1798.2(b) provides that “[a] person or business that maintains
21 computerized data that includes personal information that the person or business does
22 not own shall notify the owner or licensee of the information of the breach of the
23 security of the data immediately following discovery, if the personal information was,
24 or is reasonably believed to have been, acquired by an unauthorized person.”

25 210. The Experian Defendants are businesses that own or license computerized
26 data that include personal information as defined by Cal. Civ. Code § 1798.80 *et seq.*

211. In the alternative, the Experian Defendants maintain computerized data that includes personal information that the Experian Defendants do not own as defined by Cal. Civ. Code § 1798.80 *et seq.*

212. Plaintiffs and the California Subclass members' PII (including but not limited to names, addresses, and Social Security numbers) includes personal information covered by Cal. Civ. Code § 1798.81.5(d)(1).

213. Because Experian reasonably believed that Plaintiffs and the California Subclass members' personal information was acquired by unauthorized persons during the Data Breach, it had an obligation to disclose the Data Breach in a timely and accurate fashion under Cal. Civ. Code § 1798.82(a), or in the alternative, under Cal. Civ. Code § 1798.82(b).

214. By failing to disclose the Data Breach in a timely and accurate manner, Experian violated Cal. Civ. Code § 1798.82.

215. As a direct and proximate result of Defendants' violations of sections 1798.81.5 and 1798.82 of the California Civil Code, Plaintiffs and the California Subclass Members suffered the damages described above, including but not limited to 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 PII.

216. Plaintiffs the California Subclass seek relief under § 1798.84 of the California Civil Code, including, but not limited to, actual damages in an amount to be proven at trial, and injunctive relief.

COUNT 9

VIOLATION OF THE CALIFORNIA CONSUMERS LEGAL REMEDIES ACT

Cal. Civ. Code § 1750, et seq.

(On Behalf of the California Subclass)

217. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

1 218. The Consumers Legal Remedies Act, California Civil Code § 1750, *et seq.*
2 (the “CLRA”) has adopted a comprehensive statutory scheme prohibiting various
3 deceptive practices in connection with the conduct of a business providing goods,
4 property, or services to consumers primarily for personal, family, or household
5 purposes. The self-declared purposes of the CLRA are to protect consumers against
6 unfair and deceptive business practices and to provide efficient and economical
7 procedures to secure such protection.

8 219. Experian is a “person” as defined by Civil Code Section 1761(c), because
9 Experian is a corporation as set forth above.

10 220. Plaintiff and Class Members are “consumers” within the meaning of Civil
11 Code Section 1761(d).

12 221. Experian performed “services,” as defined by California Civil Code
13 Section 1761(a), with respect to its compilation, maintenance, use, and furnishing of
14 Plaintiffs’ and California Subclass members’ PII that was compromised in the Data
15 Breach.

16 222. Experian’s sale of their services to T-Mobile in California constitutes
17 “transaction[s]” which were “intended to result or which result[ed] in the sale” of
18 services to consumers within the meaning of Civil Code Sections 1761(e) and 1770(a).

19 223. Plaintiffs have standing to pursue this claim as they have suffered injury in
20 fact and have lost money as a result of Experian’s actions as set forth herein.

21 Specifically, Plaintiffs’ PII has been compromised and they are imminently threatened
22 with financial and identity theft, and, in fact, many have already suffered actual fraud.

23 224. Section 1770(a)(5) of the CLRA prohibits anyone from “[r]epresenting that
24 goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits,
25 or quantities which they do not have” Experian represented that its credit
26 background check services would adequately secure Plaintiffs’ and California Subclass
27 members’ PII when in fact its computer systems were inadequately protected and
28 susceptible to breach.

1 225. Section 1770(a)(7) of the CLRA prohibits anyone from “[r]epresenting that
2 goods or services are of a particular standard, quality, or grade, or that goods are of a
3 particular style or model, if they are of another.” Experian represented that its credit
4 background check services would adequately secure Plaintiffs’ and California Subclass
5 members’ PII when in fact its computer systems were inadequately protected and
6 susceptible to breach.

7 226. Section 1770(a)(9) of the CLRA prohibits anyone from “[a]dvertising
8 goods or services with intent not to sell them as advertised.” As noted above, Experian
9 failed to provide adequate security to the PII it was entrusted to secure for the purposes
10 of conducting credit background checks.

11 227. A written pre-suit demand under Cal. Civ. Code § 1782(a) is unnecessary
12 and unwarranted because Experian has long had notice of Plaintiffs’ allegations, claims
13 and demands, including from the filing of numerous underlying actions against it arising
14 from the Data Breach, the first of which were filed on or about October 2, 2015.
15 Further, Experian is the party with the most knowledge of the underlying facts giving
16 rise to Plaintiffs’ allegations, so that any pre-suit notice would not put Experian in a
17 better position to evaluate those claims.

18 228. Plaintiffs, individually and on behalf of the California Subclass, seek
19 damages, an order enjoining the acts and practices described above, and attorneys’ fees
20 and costs under the CLRA.

21 **iv. Colorado**

22 **COUNT 10**

23 **VIOLATION OF THE COLORADO CONSUMER PROTECTION ACT**

24 **Colo. Rev. Stat. § 6-1-101, *et. seq.***

25 **(On Behalf of the Colorado Subclass)**

26 229. Plaintiffs incorporate by reference all paragraphs above as if fully set forth
27 herein.
28

1 230. Experian, while operating in Colorado, engaged in deceptive practices in
2 the course of its business, vocation, and occupation, in violation of C.R.S. §6-1-105.
3 This includes, but is not limited to the following:

4 a. Experian failed to enact adequate privacy and security measures to
5 protect the Colorado Subclass members' PII from unauthorized disclosure, release, data
6 breaches, and theft, which was a direct and proximate cause of the Data Breach;

7 b. Experian failed to take proper action following known security risks
8 and prior cybersecurity incidents, which was a direct and proximate cause of the Data
9 Breach;

10 c. Experian knowingly and fraudulently misrepresented that they would
11 maintain adequate data privacy and security practices and procedures to safeguard
12 Colorado Subclass members' PII from unauthorized disclosure, release, data breaches,
13 and theft, in violation of Colo. Rev. Stat. §6-1-105(e), (g) and (u);

14 d. Experian knowingly and fraudulently misrepresented that they did
15 and would comply with the requirements of relevant federal and state laws pertaining to
16 the privacy and security of Colorado Subclass members' PII, in violation of Colo. Rev.
17 Stat. §6-1-105(e), (g) and (u);

18 e. Experian knowingly omitted, suppressed, and concealed the
19 inadequacy of the privacy and security protections for Colorado Class members' PII, in
20 violation of Colo. Rev. Stat. §6-1-105(1)(e), (g) and (u); and

21 f. Experian failed to maintain the privacy and security of Plaintiffs' and
22 the Colorado Subclass members' PII, in violation of duties imposed by applicable
23 federal and state laws, including but not limited to the FCRA, 15 U.S.C. § 1681e, and
24 the GLBA, 15 U.S.C. § 6801 *et seq.*, which was a direct and proximate cause of the
25 Data Breach.

26 g. Experian failed to disclose the Data Breach to the Colorado Subclass
27 members in a timely and accurate manner, in violation of the duties imposed by Colo.
28 Rev. Stat. Ann § 6-1-716(2).

1 231. As a direct and proximate result of Defendants' practices, the Colorado
2 Subclass members suffered injuries to legally protected interests, as described above,
3 including their legally protected interest in the confidentiality and privacy of their PII,
4 time and expenses related to monitoring their financial accounts for fraudulent activity,
5 an increased, imminent risk of fraud and identity theft, and loss of value of their PII.

6 232. The above unfair and deceptive practices and acts by Experian were
7 immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury
8 to consumers that these consumers could not reasonably avoid; this substantial injury
9 outweighed any benefits to consumers or to competition.

10 233. Experian knew or should have known that data security practices and
11 infrastructure were inadequate to safeguard the PII of members of the Colorado
12 Subclass, and that risk of a data breach or theft was highly likely. Defendants' actions in
13 engaging in the above-named unfair practices and deceptive acts were negligent,
14 knowing and willful, and/or wanton and reckless with respect to the rights of the
15 Colorado Subclass members.

16 234. Pursuant to Colo. Rev. Stat. § 6-1-113, Plaintiffs, individually and on
17 behalf of the Colorado Subclass, seek monetary relief against Defendants measured as
18 the greater of (a) actual damages in an amount to be determined at trial and
19 discretionary trebling of such damages, or (b) statutory damages in the amount of \$500
20 for each Plaintiff and each Colorado Subclass member.

21 235. Plaintiffs also seek an order enjoining Defendants' unfair, unlawful, and/or
22 deceptive practices, declaratory relief, attorneys' fees, and any other just and proper
23 relief available under the Colorado Consumer Protection Act, Colo. Rev. Stat § 6-1-101,
24 *et seq.*

25
26 ///

27
28 ///

COUNT 11

**VIOLATION OF THE COLORADO SECURITY BREACH NOTIFICATION
ACT**

Colo. Rev. Stat. Ann. § 6-1-716, *et. seq.*

(On Behalf of the Colorado Subclass)

236. Plaintiffs incorporate by reference all paragraphs above as though fully set forth herein.

237. Under Colo. Rev. Stat. Ann. § 6-1-716(2)(a), “a commercial entity that conducts business in Colorado and that owns or licenses computerized data that includes personal information about a resident of Colorado shall, when it becomes aware of a breach of the security of the system, conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused ... [and] give notice as soon as possible to the affected Colorado resident”

238. Under Colo. Rev. Stat. Ann. § 6-1-716(2)(b), “a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any breach of the security of the system immediately following discovery of a breach”

239. The Experian Defendants are businesses that own or license computerized data that includes personal information as defined by Colo. Rev. Stat. Ann. § 6-1-716.

240. In the alternative, the Experian Defendants maintain computerized data that includes personal information that the Experian Defendants do not own as defined by Colo. Rev. Stat. Ann. § 6-1-716.

241. Plaintiffs and the Colorado Subclass members’ PII (*e.g.*, Social Security numbers) includes personal information covered by Colo. Rev. Stat. Ann. § 6-1-716(1).

242. Because Experian was aware of a breach in its security system, it had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Colo. Rev. Stat. Ann. § 6-1-716 (2).

243. By failing to disclose the Data Breach in a timely and accurate manner, Experian violated Colo. Rev. Stat. Ann. § 6-1-716 (2).

244. As a direct and proximate result of Experian's violations of Colo. Rev. Stat. Ann. § 6-1-716(2), Plaintiffs and the Colorado Subclass members suffered the damages alleged herein.

245. Plaintiffs and the Colorado Subclass members seek relief under Colo. Rev. Stat. Ann. § 6-1-716(4), including, but not limited to, actual damages (to be proven at trial) and equitable relief.

v. Delaware

COUNT 12

VIOLATION OF THE DELAWARE CONSUMER FRAUD ACT

6 Del. Code § 2513, *et seq.*

(On Behalf of the Delaware Subclass)

246. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

247. Experian, while operating in Delaware, used and employed deception, fraud, 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 services, in violation of 6 Del. Code § 2513(a). This includes but is not limited the following:

a. Experian failed to enact adequate privacy and security measures to protect the Delaware Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Experian failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Experian knowingly and fraudulently misrepresented that they would maintain adequate data privacy and security practices and procedures to safeguard the

1 Delaware Subclass members' PII from unauthorized disclosure, release, data breaches,
2 and theft;

3 d. Experian knowingly omitted, suppressed, and concealed the
4 inadequacy of its privacy and security protections for the Delaware Subclass members'
5 PII;

6 e. Experian knowingly and fraudulently misrepresented that they would
7 comply with the requirements of relevant federal and state laws pertaining to the privacy
8 and security of the Delaware Subclass members' PII, including but not limited to duties
9 imposed by the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801 *et seq.*;

10 f. Experian failed to maintain the privacy and security of the Delaware
11 Subclass members' PII, in violation of duties imposed by applicable federal and state
12 laws, including but not limited to those mentioned in the aforementioned paragraph,
13 which was a direct and proximate cause of the Data Breach; and

14 g. Experian failed to disclose the Data Breach to the Delaware Subclass
15 members in a timely and accurate manner, in violation of 6 Del. Code § 12B-102(a).

16 248. As a direct and proximate result of Experian's practices, the Delaware
17 Subclass members suffered the injury and/or damages described herein, including but
18 not limited to time and expenses related to monitoring their financial accounts for
19 fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of
20 value of their PII.

21 249. The above unfair and deceptive practices and acts by Experian were
22 immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury
23 to the Delaware Subclass members that they could not reasonably avoid; this substantial
24 injury outweighed any benefits to consumers or to competition.

25 250. Experian knew or should have known that their computer systems and data
26 security practices were inadequate to safeguard the Delaware Subclass members' PII
27 and that the risk of a data breach or theft was highly likely. Experian's actions were
28

1 negligent, knowing and willful, and/or wanton and reckless with respect to the rights of
2 members of the Delaware Subclass members.

3 251. Plaintiffs and the Delaware Subclass Members seek damages under 6 Del.
4 Code § 2525 for injury resulting from the direct and natural consequences of
5 Defendants' unlawful conduct, in an amount to be proven at trial. *See also Stephenson v.*
6 *Capano Dev., Inc.*, 462 A.2d 1069, 1077 (Del. 1983). Plaintiffs and Delaware Subclass
7 members also seek an order enjoining Experian's unfair, unlawful, and/or deceptive
8 practices, declaratory relief, attorneys' fees (pursuant to 6 Del. Code § 2526) , and any
9 other just and proper relief available under the Delaware Consumer Fraud Act, 6 Del.
10 Code § 2513, *et seq.*

11 **COUNT 13**

12 **VIOLATION OF THE DELAWARE COMPUTER SECURITY BREACH ACT**

13 **6 Del. Code § 12B-102, *et seq.***

14 **(On Behalf of the Delaware Subclass)**

15 252. Plaintiffs incorporate by reference all paragraphs above as if fully set forth
16 herein.

17 253. Under Del. Code Ann. Tit. 6 § 12b-102(a), "a commercial entity that
18 conducts business in Delaware and that owns or licenses computerized data that
19 includes personal information about a resident of Delaware shall, when it becomes
20 aware of a breach of the security of the system ... give notice as soon as possible to the
21 affected Delaware resident. Notice must be made in the most expedient time possible
22 and without unreasonable delay."

23 254. Under Del. Code Ann. Tit. 6 § 12b-102(b), "a commercial entity that
24 maintains computerized data that includes personal information that the individual or
25 the commercial entity does not own or license shall give notice to and cooperate with
26 the owner or licensee of the information of any breach of the security of the system
27 immediately following discovery of a breach"
28

1 255. Each of the Experian Defendants are businesses that own or license
2 computerized data that includes personal information as defined by 6 Del. Code Ann. §
3 12B-101, *et seq.*

4 256. In the alternative, the Experian Defendants maintain computerized data that
5 includes personal information that the Experian Defendants do not own as defined by 6
6 Del. Code Ann. § 12B-101, *et seq.*

7 257. Plaintiffs and the Delaware Subclass members' PII (including but not
8 limited to names, addresses, and Social Security numbers) includes personal
9 information covered under 6 Del. Code Ann. § 12B-101(4).

10 258. Because Experian was aware of a breach of its security system that was
11 reasonably likely to result in a misuse Delaware residents' personal information,
12 Experian had an obligation to disclose the Data Breach in a timely and accurate fashion
13 pursuant to 6 Del. Code Ann. § 12B-102.

14 259. By failing to disclose the Data Breach in a timely and accurate manner,
15 Experian violated 6 Del. Code Ann. § 12B-102.

16 260. As a direct and proximate result of Experian's violations of 6 Del. Code
17 Ann. § 12B-102(a), Plaintiffs and the Delaware Subclass members suffered the damages
18 alleged herein.

19 261. Plaintiffs and the Delaware Subclass members seek relief under 6 Del.
20 Code Ann. § 12B-104, including, but not limited to, actual damages and broad equitable
21 relief.

22
23 ///

24
25 ///

26
27 ///

vi. District of Columbia

COUNT 14

**VIOLATION OF THE DISTRICT OF COLUMBIA CONSUMER PROTECTION
PROCEDURES ACT,**

D.C. Code § 28-3904, *et seq.*

(On Behalf of the District of Columbia Subclass)

262. Plaintiffs incorporate by reference all paragraphs above as if fully set forth here.

263. As defined by D.C. Code § 28-3901, D.C. Subclass members are “consumers” who did or would have purchased or received consumer goods or services, and who otherwise provide economic demand for Experian’s services.

264. Experian, while operating in the District of Columbia, used and employed deception, fraud, 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 services, in violation of D.C. Code § 28-3904. This includes but is not limited the following:

a. Experian failed to enact adequate privacy and security measures to protect the D.C. Subclass members’ PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Experian failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Experian knowingly and fraudulently misrepresented that they would maintain adequate data privacy and security practices and procedures to safeguard the D.C. Subclass members’ PII from unauthorized disclosure, release, data breaches, and theft;

d. Experian knowingly omitted, suppressed, and concealed the inadequacy of its privacy and security protections for the D.C. Subclass members’ PII;

1 e. Experian knowingly and fraudulently misrepresented that they would
2 comply with the requirements of relevant federal and state laws pertaining to the privacy
3 and security of the D.C. Subclass members' PII, including but not limited to duties
4 imposed by the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801 *et seq.*;

5 f. Experian failed to maintain the privacy and security of the D.C.
6 Subclass members' PII, in violation of duties imposed by applicable federal and state
7 laws, including but not limited to those mentioned in the aforementioned paragraph,
8 which was a direct and proximate cause of the Data Breach; and

9 g. Experian failed to disclose the Data Breach to D.C. Subclass
10 members in a timely and accurate manner, in violation of D.C. Code § 28-3852(a)

11 265. As a direct and proximate result of Experian's practices, the D.C. Subclass
12 members suffered the injury and/or damages described herein, including but not limited
13 to time and expenses related to monitoring their financial accounts for fraudulent
14 activity, an increased, imminent risk of fraud and identity theft, and loss of value of
15 their PII.

16 266. The above unfair and deceptive practices and acts by Experian were
17 immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury
18 to the D.C. Subclass members that they could not reasonably avoid; this substantial
19 injury outweighed any benefits to consumers or to competition.

20 267. Experian knew or should have known that its computer systems and data
21 security practices were inadequate to safeguard D.C. Class members' PII and that risk of
22 a data breach or theft was highly likely. Experian's actions in engaging in the above-
23 named unfair practices and deceptive acts were negligent, knowing and willful, and/or
24 wanton and reckless with respect to the rights of members of the D.C. Class.

25 268. Plaintiffs and D.C. Subclass members seek relief under D.C. Code § 28-
26 3905(k), including, but not limited to, restitution, injunctive relief, punitive damages,
27 attorneys' fees and costs, and treble damages or \$1,500 per violation, whichever is
28 greater.

COUNT 15

**VIOLATION OF THE DISTRICT OF COLUMBIA CONSUMER SECURITY
BREACH NOTIFICATION ACT,**

D.C. Code § 28-3851, *et. seq.*

(On Behalf of the District of Columbia Subclass)

269. Plaintiffs incorporate by reference all paragraphs above as if fully set forth here.

270. Experian is required to accurately notify Plaintiffs and D.C. Subclass members if it becomes aware of a breach of their data security system in the most expedient time possible and without unreasonable delay under D.C. Code § 28-3852(a).

271. Experian owns or licenses computerized data that includes personal information as defined by D.C. Code § 28-3852(a).

272. Plaintiffs and D.C. Subclass members' PII (including but not limited to names, addresses, and Social Security numbers) includes personal information as covered under D.C. Code § 28-3851(3).

273. Because Experian was aware of a breach of its security system that was reasonably likely to result in a misuse D.C. residents' personal information, Experian had an obligation to disclose the Data Breach in a timely and accurate fashion under D.C. Code § 28-3852(a).

274. By failing to disclose the Data Breach in the most expedient time possible and without unreasonable delay, Experian violated D.C. Code § 28-3852(a).

275. As a direct and proximate result of Experian's violations of D.C. Code § 28-3852, Plaintiffs and the D.C. Subclass members suffered the damages alleged herein.

276. Plaintiffs and the D.C. Subclass members seek relief under D.C. Code § 28-3853(a), including, but not limited to, actual damages and broad equitable relief.

vii. Florida

COUNT 16

**VIOLATION OF THE FLORIDA UNFAIR AND DECEPTIVE TRADE
PRACTICES ACT**

Fla. Stat. § 501.201, *et seq.*

(On Behalf of the Florida Subclass)

277. Plaintiffs incorporate by reference all paragraphs above as if fully set forth here.

278. Experian, while operating in Florida, engaged in unconscionable, unfair, and deceptive acts and practices in the conduct of trade and commerce, in violation of Fla. Stat. § 501.204(1). This includes but is not limited the following:

a. Experian failed to enact adequate privacy and security measures to protect the Florida Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Experian failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Experian knowingly and fraudulently misrepresented that they would maintain adequate data privacy and security practices and procedures to safeguard the Florida Subclass members' PII from unauthorized disclosure, release, data breaches, and theft;

d. Experian knowingly omitted, suppressed, and concealed the inadequacy of its privacy and security protections for the Florida Subclass members' PII;

e. Experian knowingly and fraudulently misrepresented that they would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Florida Subclass members' PII, including but not limited to duties

1 imposed by the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801 *et seq.*, and
2 Fla. Stat. § 501.171(2);

3 f. Experian failed to maintain the privacy and security of the Florida
4 Subclass members' PII, in violation of duties imposed by applicable federal and state
5 laws, including but not limited to those mentioned in the aforementioned paragraph,
6 which was a direct and proximate cause of the Data Breach; and

7 g. Experian failed to disclose the Data Breach to the Florida Subclass
8 members in a timely and accurate manner, in violation of Fla. Stat. § 501.171(4).

9 279. As a direct and proximate result of Experian's practices, the Florida
10 Subclass members suffered the injury and/or damages described herein, including but
11 not limited to time and expenses related to monitoring their financial accounts for
12 fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of
13 value of their PII.

14 280. The above unfair and deceptive practices and acts by Experian were
15 immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury
16 to the Florida Subclass members that they could not reasonably avoid; this substantial
17 injury outweighed any benefits to consumers or to competition.

18 281. Experian knew or should have known that their computer systems and data
19 security practices were inadequate to safeguard the Florida Subclass members' PII and
20 that the risk of a data breach or theft was highly likely. Experian's actions were
21 negligent, knowing and willful, and/or wanton and reckless with respect to the rights of
22 members of the Florida Subclass members.

23 282. Plaintiffs and the Florida Subclass seek actual damages under Fla. Stat. §
24 501.211(2), and attorneys' fees under Fla. Stat. § 501.2105(1), to be proven at trial.

25 283. Plaintiffs also seek an order enjoining Defendants' unfair, unlawful, and/or
26 deceptive practices, declaratory relief, and any other just and proper relief available
27 under the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. § 501.201, *et seq.*
28

viii. Georgia

COUNT 17

VIOLATION OF THE GEORGIA FAIR BUSINESS PRACTICES ACT

Ga. Code Ann. § 10-1-390, *et seq.*

(On Behalf of the Georgia Subclass)

284. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

285. Experian, while operating in Georgia, engaged in unfair and deceptive consumer acts in the conduct of trade and commerce, in violation of Ga. Code Ann. § 10-1-390(a), and (b). This includes but is not limited the following:

a. Experian failed to enact adequate privacy and security measures to protect the Georgia Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Experian failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Experian knowingly and fraudulently misrepresented that they would maintain adequate data privacy and security practices and procedures to safeguard the Georgia Subclass members' PII from unauthorized disclosure, release, data breaches, and theft;

d. Experian knowingly omitted, suppressed, and concealed the inadequacy of its privacy and security protections for the Georgia Subclass members' PII;

e. Experian knowingly and fraudulently misrepresented that they would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the Georgia Subclass members' PII, including but not limited to duties imposed by the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801 *et seq.*;

1 f. Experian failed to maintain the privacy and security of the Georgia
2 Subclass members' PII, in violation of duties imposed by applicable federal and state
3 laws, including but not limited to those mentioned in the aforementioned paragraph,
4 which was a direct and proximate cause of the Data Breach; and

5 g. Experian failed to disclose the Data Breach to the Georgia Subclass
6 members in a timely and accurate manner, in violation of § Ga. Code Ann 10-1-912.

7 286. As a direct and proximate result of Experian's practices, the Georgia
8 Subclass members suffered the injury and/or damages described herein, including but
9 not limited to time and expenses related to monitoring their financial accounts for
10 fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of
11 value of their PII.

12 287. The above unfair and deceptive practices and acts by Experian were
13 immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury
14 to the Georgia Subclass members that they could not reasonably avoid; this substantial
15 injury outweighed any benefits to consumers or to competition.

16 288. Experian knew or should have known that their computer systems and data
17 security practices were inadequate to safeguard the Georgia Subclass members' PII and
18 that the risk of a data breach or theft was highly likely. Experian's actions were
19 negligent, knowing and willful, and/or wanton and reckless with respect to the rights of
20 members of the Georgia Subclass members.

21 289. A written pre-suit demand under Ga. Code Ann. § 10-1-399(b) is
22 unnecessary and unwarranted because Experian has long had notice of Plaintiffs'
23 allegations, claims and demands, including from the filing of numerous underlying
24 actions against it arising from the Data Breach, the first of which were filed on or about
25 October 2, 2015. Further, Experian is the party with the most knowledge of the
26 underlying facts giving rise to Plaintiffs' allegations, so that any pre-suit notice would
27 not put Experian in a better position to evaluate those claims.
28

290. Plaintiffs and the Georgia Subclass seek damages and treble damages (for intentional violations), to be proven at trial, under Ga. Code. Ann. § 10-1-399(a) and (c).

291. Plaintiffs also seek an order enjoining Experian's unfair, unlawful, and/or deceptive practices, attorneys' fees, and any other just and proper relief available under Ga. Code. Ann. § 10-1-399.

COUNT 18

VIOLATION OF THE GEORGIA SECURITY BREACH NOTIFICATION ACT

Ga. Code Ann. § 10-1-912, *et seq.*

(On Behalf of the Georgia Subclass)

292. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

293. Under Ga. Code Ann. § 10-1-912(a), “[a]ny information broker ... that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notice shall be made in the most expedient time possible and without unreasonable delay”

294. Under Ga. Code Ann. § 10-1-912(b), “[a]ny person or business that maintains computerized data on behalf of an information broker ... that includes personal information of individuals that the person or business does not own shall notify the information broker ... of any breach of the security of the system within 24 hours following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”

295. The Experian Defendants are information brokers that own or license computerized data that includes personal information, as defined by Ga. Code Ann. § 10-1-911.

1 296. In the alternative, the Experian Defendants maintain computerized data on
2 behalf of an information broker that includes personal information that the Experian
3 Defendants do not own, as defined by Ga. Code Ann. § 10-1-911.

4 297. Plaintiffs and the Georgia Subclass members' PII (including but not limited
5 to names, addresses, and Social Security numbers) includes personal information
6 covered under Ga. Code Ann. § 10-1-911(6).

7 298. Because Experian was aware of a breach of its security system (that was
8 reasonably likely to have caused unauthorized persons to acquire Plaintiffs and Class
9 members' PII), Experian had an obligation to disclose the Data Breach in a timely and
10 accurate fashion as mandated by Ga. Code Ann. § 10-1-912(a).

11 299. By failing to disclose the Data Breach in a timely and accurate manner,
12 Experian violated Ga. Code Ann. § 10-1-912(a).

13 300. As a direct and proximate result of Experian's violations of Ga. Code Ann.
14 § 10-1-912(a), Plaintiffs and Georgia Subclass members suffered the damages alleged
15 herein.

16 301. Plaintiffs and the Georgia Subclass members seek relief under Ga. Code
17 Ann. § 10-1-912 including, but not limited to, actual damages and injunctive relief.

18 **ix. Hawaii**

19 **COUNT 19**

20 **VIOLATION OF THE HAWAII UNFAIR PRACTICES AND UNFAIR**
21 **COMPETITION STATUTE**

22 **Haw. Rev. Stat. § 480-1, *et seq.***

23 **(On Behalf of the Hawaii Subclass)**

24 302. Plaintiffs incorporate by reference all paragraphs above as if fully set forth
25 herein.

26 303. The Hawaii Subclass members are "consumers" under Haw. Rev. Stat. §
27 480-1.
28

1 304. Experian, while operating in Hawaii, engaged in unfair and deceptive acts
2 or practices, in violation of Haw. Rev. Stat. § 480- 2(a). This includes but is not limited
3 the following:

4 a. Experian failed to enact adequate privacy and security measures to
5 protect the Hawaii Subclass members' PII from unauthorized disclosure, release, data
6 breaches, and theft, which was a direct and proximate cause of the Data Breach;

7 b. Experian failed to take proper action following known security risks
8 and prior cybersecurity incidents, which was a direct and proximate cause of the Data
9 Breach;

10 c. Experian knowingly and fraudulently misrepresented that they would
11 maintain adequate data privacy and security practices and procedures to safeguard the
12 Hawaii Subclass members' PII from unauthorized disclosure, release, data breaches, and
13 theft;

14 d. Experian knowingly omitted, suppressed, and concealed the
15 inadequacy of its privacy and security protections for Hawaii Subclass members' PII;

16 e. Experian knowingly and fraudulently misrepresented that they would
17 comply with the requirements of relevant federal and state laws pertaining to the privacy
18 and security of the Hawaii Subclass members' PII, including but not limited to duties
19 imposed by the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801 *et seq.*, and
20 Hawaii's Privacy of Consumer Financial Information statute, Haw. Rev. Stat. § 431:3A-
21 101, *et seq.*;

22 f. Experian failed to maintain the privacy and security of the Hawaii
23 Subclass members' PII, in violation of duties imposed by applicable federal and state
24 laws, including but not limited to those mentioned in the aforementioned paragraph,
25 which was a direct and proximate cause of the Data Breach; and

26 g. Experian failed to disclose the Data Breach to the Hawaii Subclass
27 members in a timely and accurate manner, in violation of Haw. Rev. Stat. § 487N-2(a).
28

305. As a direct and proximate result of Experian's practices, the Hawaii Subclass members suffered the injury and/or damages described herein, including but not limited to 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 PII.

306. The above unfair and deceptive practices and acts by Experian were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to the Hawaii Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

307. Experian knew or should have known that their computer systems and data security practices were inadequate to safeguard the Hawaii Subclass members' PII and that the risk of a data breach or theft was highly likely. Experian's actions were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Hawaii Subclass members.

308. Plaintiffs and the Hawaii Subclass members seek relief under Haw. Rev. Stat. § 480-13, including, but not limited to, damages (to be proven at trial), injunctive relief, attorneys' fees and costs, and treble damages.

COUNT 20

VIOLATION OF THE HAWAII SECURITY BREACH NOTIFICATION ACT

Haw. Rev. Stat. § 487N-1, *et seq.*

(On Behalf of the Hawaii Subclass)

309. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

310. Under Haw. Rev. Stat. § 487N-2(a), “[a]ny business that owns or licenses personal information of residents of Hawaii, [or] any business that conducts business in Hawaii that owns or licenses personal information in any form (whether computerized, paper, or otherwise), ... shall provide notice to the affected person that there has been a

1 security breach following discovery or notification of the breach. The disclosure
2 notification shall be made without unreasonable delay”

3 311. Under Haw. Rev. Stat. § 487N-2(b), “[a]ny business located in Hawaii or
4 any business that conducts business in Hawaii that maintains or possesses records or
5 data containing personal information of residents of Hawaii that the business does not
6 own or license ... shall notify the owner or licensee of the information of any security
7 breach immediately following discovery of the breach”

8 312. The Experian Defendants are businesses that conduct business in Hawaii
9 and own or license computerized data of Hawaii residents that includes personal
10 information, as defined by Haw. Rev. Stat. § 487N-2(a).

11 313. In the alternative, the Experian Defendants are business that conduct
12 business in Hawaii and maintain or possess records or data containing personal
13 information of residents of Hawaii that the Experian Defendants do not own, as defined
14 by Haw. Rev. Stat. § 487N-2 (b).

15 314. Plaintiffs and the Hawaii Subclass members’ PII (including but not limited
16 to names, addresses, and Social Security numbers) includes personal information
17 covered under Haw. Rev. Stat. § 487N-1.

18 315. Because Experian was aware of a breach of its security system, Experian
19 had an obligation to disclose the Data Breach in a timely and accurate fashion under
20 Haw. Rev. Stat. § 487N-2.

21 316. By failing to disclose the Data Breach in a timely and accurate manner,
22 Experian violated Haw. Rev. Stat. § 487N-2.

23 317. As a direct and proximate result Experian’s violations of Haw. Rev. Stat. §
24 487N-2, Plaintiffs and the Hawaii Subclass members suffered the damages alleged
25 herein.

26 318. Plaintiffs and the Hawaii Subclass members seek relief under Haw. Rev.
27 Stat. § 487N-3(b), including, but not limited to, actual damages.
28

x. Illinois

COUNT 21

VIOLATION OF THE ILLINOIS CONSUMER FRAUD ACT

815 Ill. Comp. Stat. 505/1, *et seq.*

(On Behalf of the Illinois Subclass)

319. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

320. Experian, while operating in Illinois, employed unfair and deceptive acts and practices, including deception and misrepresentation, in the conduct of trade or commerce, in violation of 815 Ill. Comp. Stat. 505/2. This includes but is not limited to the following:

a. Experian failed to enact adequate privacy and security measures to protect the Illinois Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Experian failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Experian knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard Illinois Subclass members' PII from unauthorized disclosure, release, data breaches, and theft;

d. Experian omitted, suppressed, and concealed the material fact of the inadequacy of its privacy and security protections for Illinois Subclass members' PII;

e. Experian knowingly and fraudulently misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Illinois Subclass members' PII, including but not limited to duties imposed by the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801 *et seq.*, 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. Experian failed to maintain the privacy and security of Illinois Subclass members' PII, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, directly and proximately causing the Data Breach;

g. Experian failed to disclose the Data Breach to Illinois Subclass members in a timely and accurate manner, in violation of the duties imposed by 815 Ill. Comp. Stat. § 530/10(a).

321. As a direct and proximate result of Experian's practices, the Illinois Subclass members suffered injuries to legally protected interests, as described above, including their legally protected interest in the confidentiality and privacy of their PII, 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 PII.

322. The above unfair and deceptive practices and acts by Experian were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury that the Illinois Subclass members could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

323. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Illinois Subclass members' PII and that risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-described unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Illinois Subclass.

324. Plaintiffs and the Illinois Subclass members seek relief under 815 Ill. Comp. Stat. 505/10a, including but not limited to damages, restitution and punitive damages (to be proven at trial), injunctive relief, and/or attorneys' fees and costs.

COUNT 22

**VIOLATION OF THE ILLINOIS UNIFORM DECEPTIVE TRADE
PRACTICES ACT**

815 Ill. Comp. Stat. § 510/2, *et seq.*

(On Behalf of the Illinois Subclass)

325. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

326. Experian, while operating in Illinois, engaged in deceptive trade practices in the course of its business and vocation, in violation of 815 Ill. Comp. Stat. § 510/2(a), including representing that its services had characteristics that they did not have, representing that its services were of a particular standard or quality when they were not, and advertising its services with intent not to sell them as advertised. This includes but is not limited to the following:

a. Experian failed to enact adequate privacy and security measures to protect the Illinois Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Experian failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Experian knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard Illinois Subclass members' PII from unauthorized disclosure, release, data breaches, and theft;

d. Experian omitted, suppressed, and concealed the material fact of the inadequacy of its privacy and security protections for Illinois Subclass members' PII;

e. Experian knowingly and fraudulently misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Illinois Subclass members' PII, including but not limited to duties

imposed by the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801 *et seq.*, Illinois laws regulating the use and disclosure of Social Security Numbers, 815 Ill. Comp. Stat. 505/2RR, and the Illinois Consumer Fraud Act, 815 Ill. Comp. Stat. 505/1 *et seq.*;

f. Experian failed to maintain the privacy and security of Illinois Subclass members' PII, in violation of duties imposed by applicable federal and state laws, including but not limited to those mentioned in the aforementioned paragraph, directly and proximately causing the Data Breach;

g. Experian failed to disclose the Data Breach to Illinois Subclass members in a timely and accurate manner, in violation of the duties imposed by 815 Ill. Comp. Stat. § 530/10(a).

327. Experian knew or should have known that its computer systems and data security practices were inadequate and engaged in negligent, knowing, and/or willful acts of deception.

328. Illinois Subclass members were likely to be damaged by the Defendants' deceptive trade practices, which Experian knew or should have known.

329. Plaintiffs and the Illinois Subclass members seek relief under 815 Ill. Comp. Stat. 510, including, but not limited to, injunctive relief and attorney's fees.

xi. Indiana

COUNT 23

VIOLATION OF THE INDIANA DECEPTIVE CONSUMER SALES ACT

Ind. Code § 24-5-0.5-3, *et seq.*

(On Behalf of the Indiana Subclass)

330. Plaintiffs incorporate by reference all paragraphs above as if fully set forth here.

331. Experian, while operating in Indiana, engaged in unfair, abusive, or deceptive acts, omissions, or practices in connection with consumer transactions, in violation of Ind. Code § 24-5-0.5-3. This includes but is not limited to the following:

1 a. Experian failed to enact adequate privacy and security measures to
2 protect the Indiana Subclass members' PII from unauthorized disclosure, release, data
3 breaches, and theft, which was a direct and proximate cause of the Data Breach;

4 b. Experian failed to take proper action following known security risks
5 and prior cybersecurity incidents, which was a direct and proximate cause of the Data
6 Breach;

7 c. Experian knowingly and fraudulently misrepresented that it would
8 maintain adequate data privacy and security practices and procedures to safeguard the
9 Indiana Subclass members' PII from unauthorized disclosure, release, data breaches,
10 and theft;

11 d. Experian omitted, suppressed, and concealed the material fact of the
12 inadequacy of its privacy and security protections for the Indiana Subclass members'
13 PII;

14 e. Experian knowingly and fraudulently misrepresented that it would
15 comply with the requirements of relevant federal and state laws pertaining to the privacy
16 and security of the Indiana Subclass members' PII, including but not limited to duties
17 imposed by the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801 *et seq.*;

18 f. Experian failed to maintain the privacy and security of the Indiana
19 Subclass members' PII, in violation of duties imposed by applicable federal and state
20 laws, including but not limited to those mentioned in the aforementioned paragraph,
21 directly and proximately causing the Data Breach; and

22 g. Experian failed to disclose the Data Breach to the Indiana Subclass
23 members in a timely and accurate manner, in violation of the duties imposed by Ind.
24 Code § 24-4.9-3.3.

25 332. As a direct and proximate result of Experian's practices, the Indiana
26 Subclass members suffered injury and/or damages, including but not limited to time and
27 expenses related to monitoring their financial accounts for fraudulent activity, an
28 increased, imminent risk of fraud and identity theft, and loss of value of their PII.

1 333. The above unfair and deceptive acts and practices and acts by Experian
2 were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial
3 injury to the Indiana Subclass members that they could not reasonably avoid; this
4 substantial injury outweighed any benefits to consumers or to competition.

5 334. Experian knew or should have known that its computer systems and data
6 security practices were inadequate to safeguard Indiana Subclass members' PII and that
7 risk of a data breach or theft was highly likely. Experian's actions in engaging in the
8 above-named unfair practices and deceptive acts were negligent, knowing and willful,
9 and/or wanton and reckless with respect to the rights of members of the Indiana
10 Subclass.

11 335. A written pre-suit demand under Ind. Code § 24-5-0.5-5(a) is unnecessary
12 and unwarranted because Experian has long had notice of Plaintiffs' allegations, claims
13 and demands, including from the filing of numerous underlying actions against it arising
14 from the Data Breach, the first of which were filed on or about October 2, 2015.
15 Further, Experian is the party with the most knowledge of the underlying facts giving
16 rise to Plaintiffs' allegations, so that any pre-suit notice would not put Experian in a
17 better position to evaluate those claims.

18 336. Plaintiffs and Indiana Subclass members seek relief under Ind. Code §24-5-
19 0.5-4, including but not limited to, treble damages or \$1,000 per violation, whichever is
20 greater. Plaintiffs and Indiana Subclass members also seek injunctive relief and
21 attorneys' fees and costs.

22
23 ///

24
25 ///

26
27 ///

xii. Kentucky

COUNT 24

**VIOLATION OF THE KENTUCKY COMPUTER SECURITY BREACH
NOTIFICATION ACT**

Ky. Rev. Stat. Ann. § 365.732, *et seq.*

(On Behalf of the Kentucky Subclass)

337. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

338. Experian is required to accurately notify Plaintiffs and Kentucky Subclass members if Experian becomes aware of a breach of its data security system (that was reasonably likely to have caused unauthorized persons to acquire Plaintiffs and Class members' PII) in the most expedient time possible and without unreasonable delay under Ky. Rev. Stat. Ann. § 365.732(2).

339. Experian is a business that holds computerized data that includes personal information as defined by Ky. Rev. Stat. Ann. § 365.732(2).

340. Plaintiffs' and Kentucky Subclass members' PII (e.g., Social Security numbers) includes personal information as covered under Ky. Rev. Stat. Ann. § 365.732(2).

341. Because Experian was aware of a breach of its security system (was reasonably likely to have caused unauthorized persons to acquire Plaintiffs and Kentucky Subclass members' PII), Experian had an obligation to disclose the data breach in a timely and accurate fashion as mandated by Ky. Rev. Stat. Ann. § 365.732(2).

342. Thus, by failing to disclose the Data Breach in a timely and accurate manner, Experian violated Ky. Rev. Stat. Ann. § 365.732(2).

343. As a direct and proximate result of Experian's violations of Ky. Rev. Stat. Ann. § 365.732(2), Plaintiffs and Kentucky Subclass members suffered damages, as described above.

344. Plaintiffs and Kentucky Subclass members seek relief under Ky. Rev. Stat. Ann. § 446.070, including, but not limited to actual damages.

xiii. Massachusetts

COUNT 25

VIOLATION OF THE MASSACHUSETTS CONSUMER PROTECTION ACT

Mass. Gen. Laws Ann. ch. 93A, § 1, *et seq.*

(On Behalf of the Massachusetts Subclass)

345. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

346. Experian operates in “trade or commerce,” as meant by Mass. Gen. Laws Ann. ch. 93A, § 1.

347. Experian, while operating in Massachusetts, engaged in deceptive and unfair acts and practices in the conduct of trade or commerce in violation of Mass. Gen. Laws Ann. ch. 93A, § 2(a). This includes but is not limited to the following:

a. Experian failed to enact adequate privacy and security measures to protect the Massachusetts Subclass members’ PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Experian failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Experian knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard the Massachusetts Subclass members’ PII from unauthorized disclosure, release, data breaches, and theft;

d. Experian omitted, suppressed, and concealed the material fact of the inadequacy of its privacy and security protections for Massachusetts Subclass members’ PII;

1 e. Experian knowingly and fraudulently misrepresented that it would
2 comply with the requirements of relevant federal and state laws pertaining to the privacy
3 and security of the Massachusetts Subclass members' PII, including but not limited to
4 duties imposed by the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801 *et seq.*,
5 the Massachusetts Right of Privacy statute, Mass. Gen. Laws Ann. ch. 214, § 1B, and
6 the Massachusetts data breach statute, Mass. Gen. Laws Ann. ch. 93H §§ 2(a), 3(a);

7 f. Experian failed to maintain the privacy and security of the
8 Massachusetts Subclass members' PII, in violation of duties imposed by applicable
9 federal and state laws, including but not limited to those mentioned in the
10 aforementioned paragraph, directly and proximately causing the Data Breach;

11 g. Experian failed to disclose the Data Breach to the Massachusetts
12 Subclass members in a timely and accurate manner, in violation of the duties imposed
13 by Mass. Gen. Laws Ann. ch. 93H, § 3(a).

14 348. As a direct and proximate result of these practices, the Massachusetts
15 Subclass members suffered injuries to legally protected interests, as described above,
16 including but not limited to their legally protected interest in the confidentiality and
17 privacy of their PII, time and expenses related to monitoring their financial accounts for
18 fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of
19 value of their PII.

20 349. The above unfair and deceptive practices and acts by Experian were
21 immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury
22 to Massachusetts Subclass members that they could not reasonably avoid; this
23 substantial injury outweighed any benefits to consumers or to competition. These acts
24 were within the penumbra of common law, statutory, or other established concepts of
25 unfairness.

26 350. Defendants knew or should have known that their computer systems and
27 data security practices were inadequate to safeguard Massachusetts Subclass members'
28 PII and that risk of a data breach or theft was highly likely. Experian's actions in

engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the Massachusetts Subclass members.

351. A written pre-suit demand under Mass. Gen. Laws Ann. Ch. 93A § 9(3) is unnecessary and unwarranted because Experian has long had notice of Plaintiffs' allegations, claims and demands, including from the filing of numerous underlying actions against it arising from the Data Breach, the first of which were filed on or about October 2, 2015. Further, Experian is the party with the most knowledge of the underlying facts giving rise to Plaintiffs' allegations, so that any pre-suit notice would not put Experian in a better position to evaluate those claims.

352. Plaintiffs, individually and on behalf of Massachusetts Subclass members, seek relief under Mass. Gen. Laws Ann. ch. 93A, § 9, including, but not limited to, actual damages, double or treble damages, injunctive and/or other equitable relief, and/or attorneys' fees and costs.

xiv. Michigan

COUNT 26

VIOLATION OF THE MICHIGAN CONSUMER PROTECTION ACT

Mich. Comp. Laws § 445.903, *et seq.*

(On Behalf of the Michigan Subclass)

353. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

354. Experian, while operating in Michigan, engaged in unfair, unconscionable, and deceptive methods, acts and practices in the conduct of trade and commerce, including representing that its services had characteristics that they did not, representing that its services were of a particular standard when they were not, and advertising its services with intent not to dispose of them as advertised, in violation of Mich. Comp. Laws § 445.903(1). This includes but is not limited to the following:

1 a. Experian failed to enact adequate privacy and security measures to
2 protect the Michigan Subclass members' PII from unauthorized disclosure, release, data
3 breaches, and theft, which was a direct and proximate cause of the Data Breach;

4 b. Experian failed to take proper action following known security risks
5 and prior cybersecurity incidents, which was a direct and proximate cause of the Data
6 Breach;

7 c. Experian knowingly and fraudulently misrepresented that it would
8 maintain adequate data privacy and security practices and procedures to safeguard the
9 Michigan Subclass members' PII from unauthorized disclosure, release, data breaches,
10 and theft;

11 d. Experian omitted, suppressed, and concealed the material fact of the
12 inadequacy of its privacy and security protections for Michigan Subclass members' PII;

13 e. Experian knowingly and fraudulently misrepresented that it would
14 comply with the requirements of relevant federal and state laws pertaining to the privacy
15 and security of the Michigan Subclass members' PII, including but not limited to duties
16 imposed by the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801 *et seq.*;

17 f. Experian failed to maintain the privacy and security of the Michigan
18 Subclass members' PII, in violation of duties imposed by applicable federal and state
19 laws, including but not limited to those mentioned in the aforementioned paragraph,
20 directly and proximately causing the Data Breach;

21 g. Experian failed to disclose the Data Breach to the Michigan Subclass
22 members in a timely and accurate manner, in violation of the duties imposed by Mich.
23 Comp. Laws Ann. § 445.72(1).

24 355. As a direct and proximate result of these practices, the Michigan Subclass
25 members suffered injuries to legally protected interests, as described above, including
26 but not limited to their legally protected interest in the confidentiality and privacy of
27 their PII, time and expenses related to monitoring their financial accounts for fraudulent
28

1 activity, an increased, imminent risk of fraud and identity theft, and loss of value of
2 their PII.

3 356. The above unfair and deceptive practices and acts by Experian were
4 immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury
5 to Michigan Subclass members that they could not reasonably avoid; this substantial
6 injury outweighed any benefits to consumers or to competition. These acts were within
7 the penumbra of common law, statutory, or other established concepts of unfairness.

8 357. Defendants knew or should have known that their computer systems and
9 data security practices were inadequate to safeguard Michigan Subclass members' PII
10 and that risk of a data breach or theft was highly likely. Experian's actions in engaging
11 in the above-named unfair practices and deceptive acts were negligent, knowing and
12 willful, and/or wanton and reckless with respect to the rights of the Michigan Subclass
13 members.

14 358. Plaintiffs and the Michigan Subclass members seek injunctive relief to
15 enjoin Experian from continuing its unfair and deceptive acts; monetary relief against
16 Experian measured as the greater of (a) actual damages in an amount to be determined
17 at trial and (b) statutory damages in the amount of \$250 for Plaintiffs and each Michigan
18 Subclass member; reasonable attorneys' fees; and any other just and proper relief
19 available under Mich. Comp. Laws § 445.911.

20 **COUNT 27**

21 **VIOLATION OF THE MICHIGAN IDENTITY THEFT PROTECTION ACT**

22 **Mich Comp. Laws § 445.72, *et seq.***

23 **(On Behalf of the Michigan Subclass)**

24 359. Plaintiffs incorporate by reference all paragraphs above as if fully set forth
25 herein.

26 360. Under Mich. Comp. Laws Ann. § 445.72(1), "a person or agency that owns
27 or licenses data that are included in a database that discovers a security breach ... shall
28 provide a notice of the security breach to each resident of this state" whose

1 “unencrypted and unredacted personal information was accessed and acquired by an
2 unauthorized person,” or whose “personal information was accessed and acquired in
3 encrypted form by a person with unauthorized access to the encryption key.”

4 361. Under Mich. Comp. Laws Ann. § 445.72(2), “a person or agency that
5 maintains a database that includes data that the person or agency does not own or
6 license that discovers a breach of the security of the database shall provide a notice to
7 the owner or licensor of the information of the security breach.”

8 362. Under Mich. Comp. Laws Ann. § 445.72 (4), “[a] person or agency shall
9 provide any notice required under this section without unreasonable delay.”

10 363. The Experian Defendants are persons that own or license data that includes
11 personal information as defined by Mich. Comp. Laws Ann. §§ 445.63(p), 445.72, *et*
12 *seq.*

13 364. In the alternative, the Experian Defendants are persons that maintain a
14 database that includes data that they do not own or license as defined by Mich. Comp.
15 Laws Ann. §§ 445.63(p), 445.72, *et seq.*

16 365. Plaintiffs and the Michigan Subclass members’ PII (including but not
17 limited to names, addresses, and Social Security numbers) includes personal
18 information covered under Mich. Comp. Laws Ann. § 445.63(q).

19 366. Because Experian discovered and had notice of a security breach where
20 unencrypted and unredacted personal information was accessed or acquired by
21 unauthorized persons, it had an obligation to disclose the Data Breach in a timely and
22 accurate fashion under Mich. Comp. Laws Ann. § 445.72(4).

23 367. By failing to disclose the Data Breach in a timely and accurate manner,
24 Experian violated Mich. Comp. Laws Ann. § 445.72(4).

25 368. As a direct and proximate result of Experian’s violations of Mich. Comp.
26 Laws Ann. § 445.72(1)-(4), Plaintiffs and the Michigan Subclass members suffered the
27 damages alleged herein.
28

1 369. Plaintiffs and Michigan Subclass members seek relief under Mich. Comp.
2 Laws Ann. § 445.72(13), including, but not limited to actual damages (to be proven at
3 trial), and a civil fine.

4 **xv. Minnesota**

5 **COUNT 28**

6 **VIOLATION OF THE MINNESOTA PREVENTION OF CONSUMER FRAUD**
7 **ACT**

8 **Minn. Stat. §§ 325F.68 & 8.31, *et. seq.***

9 **(On Behalf of the Minnesota Subclass)**

10 370. Plaintiffs incorporate by reference all paragraphs above as if fully set forth
11 herein.

12 371. Experian, while operating in Minnesota, employed misrepresentation,
13 misleading statements, and deceptive practices, with intent that others rely thereon, in
14 connection with the sale of services, in violation of Minn. Stat. Ann. § 325F.69. This
15 includes, but is not limited to the following:

16 a. Experian failed to enact adequate privacy and security measures to
17 protect the Minnesota Subclass members' PII from unauthorized disclosure, release,
18 data breaches, and theft, which was a direct and proximate cause of the Data Breach;

19 b. Experian failed to take proper action following known security risks
20 and prior cybersecurity incidents, which was a direct and proximate cause of the Data
21 Breach;

22 c. Experian knowingly and fraudulently misrepresented that it would
23 maintain adequate data privacy and security practices and procedures to safeguard the
24 Minnesota Subclass members' PII from unauthorized disclosure, release, data breaches,
25 and theft;

26 d. Experian omitted, suppressed, and concealed the material fact of the
27 inadequacy of its privacy and security protections for the Minnesota Subclass
28 members' PII;

1 e. Experian knowingly and fraudulently misrepresented that it would
2 comply with the requirements of relevant federal and state laws pertaining to the privacy
3 and security of the Minnesota Subclass members' PII, including but not limited to duties
4 imposed by the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801 *et seq.*;

5 f. Experian failed to maintain the privacy and security of the Minnesota
6 Subclass members' PII, in violation of duties imposed by applicable federal and state
7 laws, including but not limited to those mentioned in the aforementioned paragraph,
8 directly and proximately causing the Data Breach;

9 g. Experian failed to disclose the Data Breach to the Minnesota
10 Subclass members in a timely and accurate manner, in violation of the duties imposed
11 by Minn. Stat. Ann. § 325E.61(1)(a).

12 372. As a direct and proximate result of Experian's unlawful practices, the
13 Minnesota Subclass members suffered injury and/or damages, including but not limited
14 to time and expenses related to monitoring their financial accounts for fraudulent
15 activity, an increased, imminent risk of fraud and identity theft, and loss of value of
16 their PII.

17 373. The above unlawful and deceptive acts and practices and acts by Experian
18 were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial
19 injury to the Minnesota Subclass members that they could not reasonably avoid; this
20 substantial injury outweighed any benefits to consumers or to competition.

21 374. Experian knew or should have known that its computer systems and data
22 security practices were inadequate to safeguard the Minnesota Subclass members' PII
23 and that risk of a data breach or theft was highly likely. Experian's actions in engaging
24 in the above-named practices and deceptive acts were negligent, knowing and willful.

25 375. Plaintiffs and the Minnesota Subclass members seek relief under Minn.
26 Stat. Ann. § 8.31, including, but not limited to, damages (to be proven at trial),
27 injunctive and/or other equitable relief, and attorneys' fees and costs.
28

376. The relief sought will provide a substantial benefit to the public. In addition to seeking the recovery of damages for out-of-pocket expenses incurred as result of the Data Breach, Plaintiffs seek injunctive and/or equitable relief that will protect Plaintiffs' and Minnesota Subclass members' personal information and identities, timely notify them of unlawful uses of their personal information, and ensure that Experian implements adequate security procedures.

COUNT 29

VIOLATION OF THE MINNESOTA UNIFORM DECEPTIVE TRADE PRACTICES ACT

Minn. Stat. § 325D.43, *et seq.*

(On Behalf of the Minnesota Subclass)

377. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

378. Experian, while operating in Minnesota, engaged in deceptive trade practices in the course of its business and vocation, in violation of Minn. Stat. § 325D.44, including representing that services had characteristics that they did not have, representing that services were of a particular standard or quality when they were not, and advertising services with intent not to sell them as advertised. This includes, but is not limited to, the following:

a. Experian failed to enact adequate privacy and security measures to protect the Minnesota Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Experian failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Experian knowingly and fraudulently misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard the

1 Minnesota Subclass members' PII from unauthorized disclosure, release, data breaches,
2 and theft;

3 d. Experian omitted, suppressed, and concealed the material fact of the
4 inadequacy of its privacy and security protections for the Minnesota Subclass
5 members' PII;

6 e. Experian knowingly and fraudulently misrepresented that it would
7 comply with the requirements of relevant federal and state laws pertaining to the privacy
8 and security of the Minnesota Subclass members' PII, including but not limited to duties
9 imposed by the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801 *et seq.*;

10 f. Experian failed to maintain the privacy and security of the Minnesota
11 Subclass members' PII, in violation of duties imposed by applicable federal and state
12 laws, including but not limited to those mentioned in the aforementioned paragraph,
13 directly and proximately causing the Data Breach;

14 g. Experian failed to disclose the Data Breach to the Minnesota
15 Subclass members in a timely and accurate manner, in violation of the duties imposed
16 by Minn. Stat. Ann. § 325E.61(1)(a).

17 379. As a direct and proximate result of Defendants' unlawful practices,
18 Minnesota Subclass members suffered injury and/or damages, including but not limited
19 to time and expenses related to monitoring their financial accounts for fraudulent
20 activity, an increased, imminent risk of fraud and identity theft, and loss of value of
21 their PII.

22 380. The above unlawful and deceptive acts and practices and acts by Experian
23 were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial
24 injury to the Minnesota Subclass members that they could not reasonably avoid; this
25 substantial injury outweighed any benefits to consumers or to competition.

26 381. Experian knew or should have known that its computer systems and data
27 security practices were inadequate to safeguard Minnesota Subclass members' PII and
28 that risk of a data breach or theft was highly likely. Defendants' actions in engaging in

1 the above-named unfair practices and deceptive acts were negligent, knowing and
2 willful, and/or wanton and reckless with respect to the rights of members of the
3 Minnesota Subclass members.

4 382. Minnesota Subclass members seek relief under Minn. Stat. § 325D.45,
5 including, but not limited to, injunctive relief and attorneys' fees and costs, and also
6 seek relief under Minn. Stat. Ann. § 8.31, including, but not limited to, damages, to be
7 proven at trial.

8 **xvi. Missouri**

9 **COUNT 30**

10 **VIOLATION OF THE MISSOURI MERCHANDISE PRACTICING ACT**

11 **Mo. Stat. § 407.010, *et seq.***

12 **(On Behalf of the Missouri Subclass)**

13 383. Plaintiffs incorporate by reference all paragraphs above as if fully set forth
14 herein.

15 384. Experian, while operating in Missouri, employed deception,
16 misrepresentation, unfair practices, and the concealment, suppression, and omission of
17 material facts in connection with the sale and advertisement of services in violation of
18 Mo. Stat. § 407.020(1). This includes, but is not limited to:

19 a. Experian failed to enact adequate privacy and security measures to
20 protect the Missouri Subclass members' PII from unauthorized disclosure, release, data
21 breaches, and theft, which was a direct and proximate cause of the Data Breach;

22 b. Experian failed to take proper action following known security risks
23 and prior cybersecurity incidents, which was a direct and proximate cause of the Data
24 Breach;

25 c. Experian knowingly and fraudulently misrepresented that it would
26 maintain adequate data privacy and security practices and procedures to safeguard the
27 Missouri Subclass members' PII from unauthorized disclosure, release, data breaches,
28 and theft;

1 d. Experian omitted, suppressed, and concealed the material fact of the
2 inadequacy of its privacy and security protections for the Missouri Subclass members’
3 PII;

4 e. Experian knowingly and fraudulently misrepresented that it would
5 comply with the requirements of relevant federal and state laws pertaining to the privacy
6 and security of the Missouri Subclass members’ PII, including but not limited to duties
7 imposed by the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801 *et seq.*, the
8 Missouri Unfair Trade Practice Act, Mo. Stat. § 375.936(4) and (6)(a), and Missouri
9 Statute § 354-525;

10 f. Experian failed to maintain the privacy and security of the Missouri
11 Subclass members’ PII, in violation of duties imposed by applicable federal and state
12 laws, including but not limited to those mentioned in the aforementioned paragraph,
13 directly and proximately causing the Data Breach;

14 g. Experian failed to disclose the Data Breach to the Missouri Subclass
15 members in a timely and accurate manner, in violation of the duties imposed by Mo.
16 Rev. Stat. § 407.1500(2)(1)(a).

17 385. As a direct and proximate result of Experian’s practices, the Missouri
18 Subclass members suffered an ascertainable loss of money or property, real or personal,
19 as described above, including the loss of their legally protected interest in the
20 confidentiality and privacy of their PII, time and expenses related to monitoring their
21 financial accounts for fraudulent activity, an increased, imminent risk of fraud and
22 identity theft, and loss of value of their PII.

23 386. The above unlawful and deceptive acts and practices and acts by Experian
24 were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial
25 injury to the Missouri Subclass members that they could not reasonably avoid; this
26 substantial injury outweighed any benefits to consumers or to competition.

27 387. Experian knew or should have known that its computer systems and data
28 security practices were inadequate to safeguard Missouri Subclass members’ PII and

1 that risk of a data breach or theft was highly likely. Experian's actions in engaging in
2 the above-named unfair practices and deceptive acts were negligent, knowing and
3 willful.

4 388. Plaintiffs and the Missouri Subclass members seek relief under Mo. Ann.
5 Stat. § 407.025, including, but not limited to, injunctive relief, actual damages, punitive
6 damages, and attorneys' fees and costs.

7 **xvii. Nevada**

8 **COUNT 31**

9 **VIOLATION OF THE NEVADA DECEPTIVE TRADE PRACTICES ACT**

10 **Nev. Rev. Stat. Ann. § 598.0915, *et seq.***

11 **(On Behalf of the Nevada Subclass)**

12 389. Plaintiffs incorporate by reference all paragraphs above as if fully set forth
13 herein.

14 390. Experian's violations of federal law, alleged above, constitute "deceptive
15 trade practices" as defined under Nevada law, including under Nev. Rev. Stat.
16 § 598.0923.

17 391. Furthermore, while operating in Nevada, Experian engaged in deceptive
18 trade practices in the course of its business and occupation, including by representing
19 that its services had characteristics that they did not have, representing that its services
20 were of a particular standard or quality when they were not, and advertising its services
21 with intent not to sell them as advertised, in violation of Nev. Rev. Stat. § 598.0915.
22 This includes but is not limited to the following:

23 a. Experian failed to enact adequate privacy and security measures to
24 protect the Nevada Subclass members' PII from unauthorized disclosure, release, data
25 breaches, and theft, which was a direct and proximate cause of the Data Breach;

26 b. Experian failed to take proper action following known security risks
27 and prior cybersecurity incidents, which was a direct and proximate cause of the Data
28 Breach;

1 c. Experian knowingly and fraudulently misrepresented that it would
2 maintain adequate data privacy and security practices and procedures to safeguard the
3 Nevada Subclass members' PII from unauthorized disclosure, release, data breaches,
4 and theft;

5 d. Experian omitted, suppressed, and concealed the material fact of the
6 inadequacy of its privacy and security protections for the Nevada Subclass members'
7 PII;

8 e. Experian knowingly and fraudulently misrepresented that it would
9 comply with the requirements of relevant federal and state laws pertaining to the privacy
10 and security of the Nevada Subclass members' PII, including but not limited to duties
11 imposed by the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801 *et seq.*; and

12 f. Experian failed to maintain the privacy and security of the Nevada
13 Subclass members' PII, in violation of duties imposed by applicable federal and state
14 laws, including but not limited to those mentioned in the aforementioned paragraph,
15 directly and proximately causing the Data Breach.

16 392. As a direct and proximate result of Experian's practices, the Nevada
17 Subclass members suffered injury and/or damages, including but not limited to time and
18 expenses related to monitoring their financial accounts for fraudulent activity, an
19 increased, imminent risk of fraud and identity theft, and loss of value of their PII.

20 393. The above unfair and deceptive acts and practices and acts by Experian
21 were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial
22 injury to the Nevada Subclass members that they could not reasonably avoid; this
23 substantial injury outweighed any benefits to consumers or to competition.

24 394. Experian knew or should have known that its computer systems and data
25 security practices were inadequate to safeguard the Nevada Subclass members' PII and
26 that risk of a data breach or theft was highly likely. Experian's actions in engaging in
27 the above-named unfair practices and deceptive acts were negligent, knowing and
28 willful.

1 395. Plaintiffs and the Nevada Subclass seek all available relief under Nev. Rev.
2 Stat. Ann. § 41.600, including but not limited to injunctive relief, other equitable relief,
3 actual damages, and attorneys' fees and costs.

4 **xviii. New Jersey**

5 **COUNT 32**

6 **VIOLATION OF THE NEW JERSEY CONSUMER FRAUD ACT**

7 **N.J. Stat. Ann. § 56:8-1, *et seq.***

8 **(On Behalf of the New Jersey Subclass)**

9 396. Plaintiffs incorporate by reference all paragraphs above as if fully set forth
10 herein.

11 397. Experian, while operating in New Jersey, engaged, in unconscionable
12 commercial practices, deception, misrepresentation, and the knowing concealment,
13 suppression, and omission of material facts with intent that others rely on such
14 concealment, suppression, and omission, in connection with the sale and advertisement
15 of services, in violation of N.J. Stat. Ann. § 56:8-2. This includes, but is not limited to
16 the following:

17 a. Experian failed to enact adequate privacy and security measures to
18 protect the New Jersey Subclass members' PII from unauthorized disclosure, release,
19 data breaches, and theft, which was a direct and proximate cause of the Data Breach;

20 b. Experian failed to take proper action following known security risks
21 and prior cybersecurity incidents, which was a direct and proximate cause of the Data
22 Breach;

23 c. Experian knowingly and fraudulently misrepresented that it would
24 maintain adequate data privacy and security practices and procedures to safeguard the
25 New Jersey Subclass members' PII from unauthorized disclosure, release, data
26 breaches, and theft;

1 d. Experian omitted, suppressed, and concealed the material fact of the
2 inadequacy of its privacy and security protections for the New Jersey Subclass
3 members' PII;

4 e. Experian knowingly and fraudulently misrepresented that it would
5 comply with the requirements of relevant federal and state laws pertaining to the privacy
6 and security of the New Jersey Subclass members' PII, including but not limited to
7 duties imposed by the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801 *et*
8 *seq.*;

9 f. Experian failed to maintain the privacy and security of the New
10 Jersey Subclass members' PII, in violation of duties imposed by applicable federal and
11 state laws, including but not limited to those mentioned in the aforementioned
12 paragraph, directly and proximately causing the Data Breach;

13 g. Experian failed to disclose the Data Breach to the New Jersey
14 Subclass members in a timely and accurate manner, in violation of the duties imposed
15 by N.J. Stat. Ann. § 56:8-163(a).

16 398. As a direct and proximate result of Experian's practices, the New Jersey
17 Subclass members suffered an ascertainable loss of money or property, real or personal,
18 as described above, including the loss of their legally protected interest in the
19 confidentiality and privacy of their PII, time and expenses related to monitoring their
20 financial accounts for fraudulent activity, an increased, imminent risk of fraud and
21 identity theft, and loss of value of their PII.

22 399. The above unlawful and deceptive acts and practices and acts by Experian
23 were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial
24 injury to the New Jersey Subclass members that they could not reasonably avoid; this
25 substantial injury outweighed any benefits to consumers or to competition.

26 400. Experian knew or should have known that its computer systems and data
27 security practices were inadequate to safeguard the New Jersey Subclass members' PII
28 and that risk of a data breach or theft was highly likely. Experian's actions in engaging

1 in the above-named unfair practices and deceptive acts were negligent, knowing and
2 willful.

3 401. Plaintiffs and the New Jersey Subclass members seek relief under N.J. Stat.
4 Ann. § 56:8-19, including, but not limited to, injunctive relief, other equitable actual
5 damages (to be proven at trial), treble damages, and attorneys' fees and costs.

6 **COUNT 33**

7 **VIOLATION OF THE NEW JERSEY CUSTOMER SECURITY BREACH**
8 **DISCLOSURE ACT**

9 **N.J. Stat. Ann. §§ 56:8-163, *et seq.***

10 **(On Behalf of the New Jersey Subclass)**

11 402. Plaintiffs incorporate by reference all paragraphs above as if fully set forth
12 herein.

13 403. Under N.J.S.A. § 56:8-163(b), “[a]ny business ... that compiles or
14 maintains computerized records that include personal information on behalf of another
15 business or public entity shall notify that business or public entity, who shall notify its
16 New Jersey customers ... of any breach of security of the computerized records
17 immediately following discovery, if the personal information was, or is reasonably
18 believed to have been, accessed by an unauthorized person.”

19 404. The Experian Defendants are businesses that compile or maintain
20 computerized records that include personal information on behalf of another business
21 under N.J.S.A. § 56:8-163(b).

22 405. Plaintiffs and the New Jersey Subclass members' PII (including but not
23 limited to names, addresses, and social security numbers) includes personal information
24 covered under N.J.S.A. §§ 56:8-163, *et seq.*

25 406. Because Experian discovered a breach of its security system in which
26 personal information was, or is reasonably believed to have been, acquired by an
27 unauthorized person and the personal information was not secured, Experian had an
28

obligation to disclose the Data Breach in a timely and accurate fashion as mandated under N.J.S.A. §§ 56:8-163, *et seq.*

407. By failing to disclose the Data Breach in a timely and accurate manner, Experian violated N.J.S.A. § 56:8-163(b).

408. As a direct and proximate result of Experian's violations of N.J.S.A. § 56:8-163(b), Plaintiffs and the New Jersey Subclass members suffered the damages described above.

409. Plaintiffs and the New Jersey Subclass members seek relief under N.J.S.A. 56:8-19, including but not limited to treble damages (to be proven at trial), attorneys' fees and costs, and injunctive relief.

xix. New Mexico

COUNT 34

VIOLATION OF THE NEW MEXICO UNFAIR PRACTICES ACT

N.M. Stat. Ann. § 57-12-2, *et seq.*

(On Behalf of the New Mexico Subclass)

410. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

411. Experian, while operating in New Mexico, engaged in deceptive trade practices in connection with the sale and advertisement of services, in violation of N.M. Stat. Ann. § 57-12-2, including by representing that its services had characteristics that they did not have, representing that its services were of a particular standard or quality when they were not, and advertising its services with intent not to sell them as advertised. This includes but is not limited to the following:

a. Experian failed to enact adequate privacy and security measures to protect the New Mexico Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

1 b. Experian failed to take proper action following known security risks
2 and prior cybersecurity incidents, which was a direct and proximate cause of the Data
3 Breach;

4 c. Experian knowingly and fraudulently misrepresented that it would
5 maintain adequate data privacy and security practices and procedures to safeguard the
6 New Mexico Subclass members' PII from unauthorized disclosure, release, data
7 breaches, and theft;

8 d. Experian omitted, suppressed, and concealed the material fact of the
9 inadequacy of its privacy and security protections for the New Mexico Subclass
10 members' PII;

11 e. Experian knowingly and fraudulently misrepresented that it would
12 comply with the requirements of relevant federal and state laws pertaining to the privacy
13 and security of the New Mexico Subclass members' PII, including but not limited to
14 duties imposed by the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801 *et*
15 *seq.*; and

16 f. Experian failed to maintain the privacy and security of the New
17 Mexico Subclass members' PII, in violation of duties imposed by applicable federal and
18 state laws, including but not limited to those mentioned in the aforementioned
19 paragraph, directly and proximately causing the Data Breach.

20 412. Experian further engaged in "unconscionable trade practices" as defined by
21 N.M. Stat. Ann. § 57-12-2, because the PII it mishandled was gathered and used for the
22 sale, or offering for sale, of services and/or for the extension of credit to Plaintiffs and
23 New Mexico Subclass members, and took advantage of Plaintiffs' and New Mexico
24 Subclass members' lack of knowledge, ability, experience, or capacity to prevent the
25 harm caused by the Data Breach, to a grossly unfair degree.

26 413. As a direct and proximate result of Experian's practices, the New Mexico
27 Subclass members suffered an ascertainable loss of money or property, real or personal,
28 as described above, including the loss of their legally protected interest in the

1 confidentiality and privacy of their PII, time and expenses related to monitoring their
2 financial accounts for fraudulent activity, an increased, imminent risk of fraud and
3 identity theft, and loss of value of their PII.

4 414. The above unlawful and deceptive acts and practices and acts by Experian
5 were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial
6 injury to the New Mexico Subclass members that they could not reasonably avoid; this
7 substantial injury outweighed any benefits to consumers or to competition.

8 415. Experian knew or should have known that its computer systems and data
9 security practices were inadequate to safeguard the New Mexico Subclass members' PII
10 and that risk of a data breach or theft was highly likely. Experian's actions in engaging
11 in the above-named unfair, unconscionable, and deceptive acts and practices were
12 negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of
13 members of the New Mexico Subclass.

14 416. Plaintiffs and the New Mexico Subclass members seek all available relief
15 under N.M. Stat. Ann. § 57-12-10, including, but not limited to, injunctive relief, actual
16 damages, and attorneys' fees and costs, as well as treble damages or \$300, whichever is
17 greater, to the Plaintiffs.

18 **xx. New York**

19 **COUNT 35**

20 **VIOLATION OF THE NEW YORK GENERAL BUSINESS LAW**

21 **N.Y. Gen. Bus. Law § 349**

22 **(On Behalf of the New York Subclass)**

23 417. Plaintiffs incorporate by reference all paragraphs above as if fully set forth
24 herein.

25 418. Experian, while operating in New York, engaged in deceptive acts and
26 practices in the conduct of business, trade and commerce, and the furnishing of services,
27 in violation of N.Y. Gen. Bus. Law § 349(a). This includes but is not limited to the
28 following:

1 a. Experian failed to enact adequate privacy and security measures to
2 protect the New York Subclass members' PII from unauthorized disclosure, release,
3 data breaches, and theft, which was a direct and proximate cause of the Data Breach;

4 b. Experian failed to take proper action following known security risks
5 and prior cybersecurity incidents, which was a direct and proximate cause of the Data
6 Breach;

7 c. Experian knowingly and fraudulently misrepresented that it would
8 maintain adequate data privacy and security practices and procedures to safeguard the
9 New York Subclass members' PII from unauthorized disclosure, release, data breaches,
10 and theft;

11 d. Experian omitted, suppressed, and concealed the material fact of the
12 inadequacy of its privacy and security protections for the New York Subclass members'
13 PII;

14 e. Experian knowingly and fraudulently misrepresented that it would
15 comply with the requirements of relevant federal and state laws pertaining to the privacy
16 and security of the New York Subclass members' PII, including but not limited to duties
17 imposed by the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801 *et seq.*;

18 f. Experian failed to maintain the privacy and security of the New York
19 Subclass members' PII, in violation of duties imposed by applicable federal and state
20 laws, including but not limited to those mentioned in the aforementioned paragraph,
21 directly and proximately causing the Data Breach;

22 g. Experian failed to disclose the Data Breach to the New York
23 Subclass members in a timely and accurate manner, in violation of the duties imposed
24 by N.Y. Gen Bus. Law § 899-aa(2).

25 419. As a direct and proximate result of Experian's practices, the New York
26 Subclass members suffered injury and/or damages, including but not limited to time and
27 expenses related to monitoring their financial accounts for fraudulent activity, an
28 increased, imminent risk of fraud and identity theft, and loss of value of their PII.

1 420. The above unfair and deceptive acts and practices and acts by Experian
2 were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial
3 injury to the New York Subclass members that they could not reasonably avoid; this
4 substantial injury outweighed any benefits to consumers or to competition.

5 421. Experian knew or should have known that its computer systems and data
6 security practices were inadequate to safeguard the New York Subclass members' PII
7 and that risk of a data breach or theft was highly likely. Experian's actions in engaging
8 in the above-named unfair practices and deceptive acts were negligent, knowing and
9 willful.

10 422. Plaintiffs and the New York Subclass members seek relief under N.Y. Gen.
11 Bus. Law § 349(h), including but not limited to actual damages (to be proven at trial),
12 treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

13 **xxi. North Carolina**

14 **COUNT 36**

15 **VIOLATION OF THE NORTH CAROLINA UNFAIR TRADE PRACTICES**
16 **ACT**

17 **N.C. Gen. Stat. Ann. § 75-1.1, *et seq.***

18 **(On Behalf of the North Carolina Subclass)**

19 423. Plaintiffs incorporate by reference all paragraphs above as if fully set forth
20 herein.

21 424. Experian, while operating in North Carolina, engaged in unfair or deceptive
22 acts and practices affecting commerce, in violation of N.C. Gen. Stat. § 75-1.1. This
23 includes but is not limited to the following:

24 a. Experian failed to enact adequate privacy and security measures to
25 protect North Carolina Subclass members' PII from unauthorized disclosure, release,
26 data breaches, and theft, which was a direct and proximate cause of the Data Breach;
27
28

1 b. Experian failed to take proper action following known security risks
2 and prior cybersecurity incidents, which was a direct and proximate cause of the Data
3 Breach;

4 c. Experian knowingly and fraudulently misrepresented that it would
5 maintain adequate data privacy and security practices and procedures to safeguard the
6 North Carolina Subclass members' PII from unauthorized disclosure, release, data
7 breaches, and theft;

8 d. Experian omitted, suppressed, and concealed the material fact of the
9 inadequacy of its privacy and security protections for North Carolina Subclass
10 members' PII;

11 e. Experian knowingly and fraudulently misrepresented that it would
12 comply with the requirements of relevant federal and state laws pertaining to the privacy
13 and security of North Carolina Subclass members' PII, including but not limited to
14 duties imposed by the FCRA, 15 U.S.C. § 1681e, the GLBA, 15 U.S.C. § 6801 *et seq.*,
15 and the North Carolina Consumer and Customer Information Privacy Act, N.C. Gen.
16 Stat. § 58-39-1, *et seq.*;

17 f. Experian failed to maintain the privacy and security of North
18 Carolina Subclass members' PII, in violation of duties imposed by applicable federal
19 and state laws, including but not limited to those mentioned in the aforementioned
20 paragraph, directly and proximately causing the Data Breach; and

21 g. Experian failed to disclose the Data Breach to North Carolina
22 Subclass members in a timely and accurate manner, in violation of duties imposed by
23 N.C. Gen. Stat. Ann. § 75-65.

24 425. As a direct and proximate result of Experian's practices, North Carolina
25 Subclass members suffered injury and/or damages, including but not limited to time and
26 expenses related to monitoring their financial accounts for fraudulent activity, an
27 increased, imminent risk of fraud and identity theft, and loss of value of their PII.
28

426. The above unfair and deceptive acts and practices and acts by Experian were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to North Carolina Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

427. Experian knew or should have known that its computer systems and data security practices were inadequate to safeguard North Carolina Subclass members' PII and that risk of a data breach or theft was highly likely. Experian's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing, willful, and/or wanton and reckless.

428. Plaintiffs and the North Carolina Subclass seek all available relief under N.C. Gen. Stat. §§ 75-16 and 75-16.1 including but not limited to injunctive relief, actual damages, treble damages, and attorneys' fees and costs.

xxii. Ohio

COUNT 37

VIOLATION OF THE OHIO CONSUMER SALES PRACTICES ACT

Ohio Rev. Code § 1345.01, *et seq.*

(On Behalf of the Ohio Subclass)

429. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

430. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

431. Experian, while operating in Ohio, engaged in unfair and deceptive acts and practices in connection with a consumer transaction, in violation of Ohio Rev. Code § 1345.01(A) and (B). This includes but is not limited to the following:

a. Experian failed to enact adequate privacy and security measures to protect the Ohio Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

1 b. Experian failed to take proper action following known security risks
2 and prior cybersecurity incidents, which was a direct and proximate cause of the Data
3 Breach;

4 c. Experian knowingly and fraudulently misrepresented that it would
5 maintain adequate data privacy and security practices and procedures to safeguard the
6 Ohio Subclass members' PII from unauthorized disclosure, release, data breaches, and
7 theft;

8 d. Experian omitted, suppressed, and concealed the material fact of the
9 inadequacy of its privacy and security protections for the Ohio Subclass members' PII;

10 e. Experian knowingly and fraudulently misrepresented that it would
11 comply with the requirements of relevant federal and state laws pertaining to the privacy
12 and security of the Ohio Subclass members' PII, including but not limited to duties
13 imposed by the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801 *et seq.*;

14 f. Experian failed to maintain the privacy and security of the Ohio
15 Subclass members' PII, in violation of duties imposed by applicable federal and state
16 laws, including but not limited to those mentioned in the aforementioned paragraph,
17 directly and proximately causing the Data Breach;

18 g. Experian failed to disclose the Data Breach to the Ohio Subclass
19 members in a timely and accurate manner, in violation of the duties imposed by Ohio
20 Rev. Code § 1349.19(B).

21 432. As a direct and proximate result of Experian's practices, the Ohio Subclass
22 members suffered injury and/or damages, including but not limited to time and expenses
23 related to monitoring their financial accounts for fraudulent activity, an increased,
24 imminent risk of fraud and identity theft, and loss of value of their PII.

25 433. The above unfair and deceptive acts and practices and acts by Experian
26 were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial
27 injury to the Ohio Subclass members that they could not reasonably avoid; this
28 substantial injury outweighed any benefits to consumers or to competition.

434. Experian knew or should have known that its computer systems and data security practices were inadequate to safeguard the Ohio Subclass members' PII and that risk of a data breach or theft was highly likely. Experian's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful.

435. Pursuant to Ohio Rev. Code § 1345.09, Plaintiffs and the Ohio Subclass members seek an order enjoining Experian's unfair and/or deceptive acts or practices actual damages – trebled (to be proven at the time of trial), and attorneys' fees, costs, and any other just and proper relief, to the extent available under the Ohio Consumer Sales Practices Act, Ohio Rev. Code §§ 1345.01, *et seq.*

COUNT 38

VIOLATION OF THE OHIO DECEPTIVE TRADE PRACTICES ACT

Ohio Rev. Code § 4165.01, *et seq.*

(On Behalf of the Ohio Subclass)

436. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

437. Experian, while operating in Ohio, engaged in deceptive trade practices in the course of its business and vocation, including representing that its services had characteristics that they did not have, representing that its services were of a particular standard or quality when they were not, and advertising its services with intent not to sell them as advertised. in violation of Ohio Rev. Code § 4165.02(A). This includes but is not limited to the following:

a. Experian failed to enact adequate privacy and security measures to protect the Ohio Subclass members' PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Experian failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach:

1 c. Experian knowingly and fraudulently misrepresented that it would
2 maintain adequate data privacy and security practices and procedures to safeguard the
3 Ohio Subclass members' PII from unauthorized disclosure, release, data breaches, and
4 theft;

5 d. Experian omitted, suppressed, and concealed the material fact of the
6 inadequacy of its privacy and security protections for the Ohio Subclass members' PII;

7 e. Experian knowingly and fraudulently misrepresented that it would
8 comply with the requirements of relevant federal and state laws pertaining to the privacy
9 and security of the Ohio Subclass members' PII, including but not limited to duties
10 imposed by the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801 *et seq.*;

11 f. Experian failed to maintain the privacy and security of the Ohio
12 Subclass members' PII, in violation of duties imposed by applicable federal and state
13 laws, including but not limited to those mentioned in the aforementioned paragraph,
14 directly and proximately causing the Data Breach;

15 g. Experian failed to disclose the Data Breach to the Ohio Subclass
16 members in a timely and accurate manner, in violation of the duties imposed by Ohio
17 Rev. Code § 1349.19(B).

18 438. As a direct and proximate result of Experian's practices, the Ohio Subclass
19 members suffered injury and/or damages, including but not limited to time and expenses
20 related to monitoring their financial accounts for fraudulent activity, an increased,
21 imminent risk of fraud and identity theft, and loss of value of their PII.

22 439. The above unfair and deceptive acts and practices and acts by Experian
23 were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial
24 injury to the Ohio Subclass members that they could not reasonably avoid; this
25 substantial injury outweighed any benefits to consumers or to competition.

26 440. Experian knew or should have known that its computer systems and data
27 security practices were inadequate to safeguard the Ohio Subclass members' PII and
28 that risk of a data breach or theft was highly likely. Experian's actions in engaging in

1 the above-named unfair practices and deceptive acts were negligent, knowing and
2 willful.

3 441. Pursuant to Ohio Rev. Code § 1345.09, Plaintiffs and the Ohio Subclass
4 members seek an order enjoining Experian's unfair and/or deceptive acts or practices
5 actual damages – trebled (to be proven at the time of trial), and attorneys' fees, costs,
6 and any other just and proper relief, to the extent available under the Ohio Consumer
7 Sales Practices Act, Ohio Rev. Code §§ 1345.01, *et seq.*

8 **xxiii. Oregon**

9 **COUNT 39**

10 **VIOLATION OF THE OREGON UNLAWFUL TRADE PRACTICES ACT**

11 **Or. Rev. Stat. § 646.608, *et seq.***

12 **(On Behalf of the Oregon Subclass)**

13 442. Plaintiffs incorporate by reference all paragraphs above as if fully set forth
14 herein.

15 443. While operating in Oregon, Experian engaged in deceptive trade practices
16 in the course of its business and occupation, including by representing that its services
17 had characteristics that they did not have, representing that its services were of a
18 particular standard or quality when they were not, advertising its services with intent not
19 to sell them as advertised, and engaging in other unfair and deceptive conduct in trade
20 or commerce, in violation of Or. Rev. Stat. § 646.608(1)(e), (g), and (u). This includes
21 but is not limited to the following:

22 a. Experian failed to enact adequate privacy and security measures to
23 protect the Oregon Subclass members' PII from unauthorized disclosure, release, data
24 breaches, and theft, which was a direct and proximate cause of the Data Breach;

25 b. Experian failed to take proper action following known security risks
26 and prior cybersecurity incidents, which was a direct and proximate cause of the Data
27 Breach;

1 c. Experian knowingly and fraudulently misrepresented that it would
2 maintain adequate data privacy and security practices and procedures to safeguard the
3 Oregon Subclass members' PII from unauthorized disclosure, release, data breaches,
4 and theft;

5 d. Experian omitted, suppressed, and concealed the material fact of the
6 inadequacy of its privacy and security protections for the Oregon Subclass members'
7 PII;

8 e. Experian knowingly and fraudulently misrepresented that it would
9 comply with the requirements of relevant federal and state laws pertaining to the privacy
10 and security of the Oregon Subclass members' PII, including but not limited to duties
11 imposed by the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801 *et seq.*;

12 f. Experian failed to maintain the privacy and security of the Oregon
13 Subclass members' PII, in violation of duties imposed by applicable federal and state
14 laws, including but not limited to those mentioned in the aforementioned paragraph,
15 directly and proximately causing the Data Breach; and

16 g. Experian violated the Oregon Consumer Identity Theft Protection
17 Act, Or. Rev. Stat. Ann. § 646A.600, *et seq.*, as alleged in more detail below.

18 444. As a direct and proximate result of Experian's practices, the Oregon
19 Subclass members suffered injury and/or damages, including but not limited to time and
20 expenses related to monitoring their financial accounts for fraudulent activity, an
21 increased, imminent risk of fraud and identity theft, and loss of value of their PII.

22 445. The above unfair and deceptive acts and practices and acts by Experian
23 were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial
24 injury to the Oregon Subclass members that they could not reasonably avoid; this
25 substantial injury outweighed any benefits to consumers or to competition.

26 446. Experian knew or should have known that its computer systems and data
27 security practices were inadequate to safeguard the Oregon Subclass members' PII and
28 that risk of a data breach or theft was highly likely. Experian's actions in engaging in

1 the above-named unfair practices and deceptive acts were negligent, knowing and
2 willful.

3 447. Plaintiffs and the Oregon Subclass seek all remedies available under Or.
4 Rev. Stat. § 646.638, including equitable relief, actual damages, statutory damages of
5 \$200 per violation, and/or punitive damages.

6 448. Plaintiffs and the Oregon Subclass also seek reasonable attorneys' fees and
7 costs under Or. Rev. Stat. § 646.638(3).

8 **COUNT 40**

9 **VIOLATION OF THE OREGON CONSUMER IDENTITY THEFT**
10 **PROTECTION ACT**

11 **Or. Rev. Stat. § 646A.600, *et seq.***

12 **(On Behalf of the Oregon Subclass)**

13 449. Plaintiffs incorporate by reference all paragraphs above as if fully set forth
14 herein.

15 450. Under Or. Rev. Stat. Ann. § 646A.622(1), a business "that maintains
16 records which contain personal information" of a Oregon resident "shall implement and
17 maintain reasonable security measures to protect those records from unauthorized
18 access, acquisition, destruction, use, modification or disclosure."

19 451. Experian is a business that maintains records which contain personal
20 information, within the meaning of Or. Rev. Stat. Ann. § 646A.622(1), about Plaintiffs
21 and Oregon Subclass members.

22 452. Experian violated Or. Rev. Stat. Ann. § 646A.622(1) by failing to
23 implement reasonable measures to protect Plaintiffs' and Oregon Subclass members'
24 PII.

25 453. Experian is required to accurately notify Plaintiffs and Oregon Subclass
26 members if Experian becomes aware of a breach of their data security system in the
27 most expeditious time possible and without unreasonable delay under Or. Rev. Stat.
28 Ann. § 646A.604(1).

1 454. Experian is a business that owns, maintains, or otherwise possesses data
2 that includes consumers personal information as defined by Or. Rev. Stat. Ann. §
3 646A.604(1).

4 455. Plaintiffs' and Oregon Subclass members' PII (e.g., Social Security
5 numbers) includes personal information as covered under Or. Rev. Stat. Ann. §
6 646A.604(1).

7 456. Because Experian discovered a breach of their security system, Experian
8 had an obligation to disclose the Data Breach in a timely and accurate fashion as
9 mandated by Or. Rev. Stat. Ann. § 646A.604(1).

10 457. As a direct and proximate result of Experian's violations of Or. Rev. Stat.
11 Ann. §§ 646A.604(1) and 646A.622(1), Plaintiffs and Oregon Subclass members
12 suffered damages, as described above.

13 458. Experian's failure to implement reasonable security measures, to promptly
14 notify Plaintiff and other Oregon Subclass members, and otherwise to comply with Or.
15 Rev. Stat. § 646A.600 *et seq.* constitutes unlawful, unfair, and deceptive practices under
16 § 646.607(9).

17 459. Plaintiffs and Oregon Subclass members seek compensation for affected
18 consumers under Or. Rev. Stat. § 646A.624(3), because enforcement of the rights of the
19 consumers through this private civil action is feasible, and not so burdensome or
20 expensive as to be impractical.

21 460. Plaintiffs and Oregon Subclass members seek relief under Or. Rev. Stat. §
22 646A.624(3), including, but not limited to, actual damages and injunctive relief.

23
24 ///

25
26 ///

27
28 ///

xxiv. Pennsylvania

COUNT 41

**VIOLATION OF THE PENNSYLVANIA UNFAIR TRADE PRACTICES AND
CONSUMER PROTECTION LAW**

73 Pa. Stat. §§ 201-2 & 201-3, *et seq.*

(On Behalf of the Pennsylvania Subclass)

461. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

462. The Pennsylvania Class members provided their PII to Experian pursuant to transactions for cellular services in “trade” and “commerce,” as meant by 73 Pa. Cons. Stat. § 201-2, for personal, family, and/or household purposes.

463. This Count is brought for Experian’s deceptive conduct, including unlawful and unfair acts and practices, which created a likelihood of confusion or of misunderstanding for Pennsylvania Class members.

464. Experian engaged in unlawful, unfair, and deceptive acts and practices with respect to the sale and advertisement of the services purchased by the Pennsylvania Class in violation of 73 Pa. Cons. Stat. Ann. § 201-3, including but not limited to the following:

a. Experian failed to enact adequate privacy and security measures to protect the Pennsylvania Subclass members’ PII from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Experian failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Experian negligently represented that it would maintain adequate data privacy and security practices and procedures to safeguard the Pennsylvania Subclass members’ PII from unauthorized disclosure, release, data breaches, and theft was deceptive given the inadequacy of its privacy and security protections;

1 d. Experian's negligence in failing to disclose the material fact of the
2 inadequacy of its privacy and security protections for the Pennsylvania Subclass
3 members' PII was deceptive;

4 e. Experian negligently represented that it would comply with the
5 requirements of relevant federal and state laws pertaining to the privacy and security of
6 the Pennsylvania Subclass members' PII, including but not limited to duties imposed by
7 the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801 *et seq.* was deceptive
8 given the inadequacy of its privacy and security protections;

9 f. Experian failed to maintain the privacy and security of the
10 Pennsylvania Subclass members' PII, in violation of duties imposed by applicable
11 federal and state laws, including but not limited to those mentioned in the
12 aforementioned paragraph, directly and proximately causing the Data Breach;

13 465. The above unlawful, unfair, and deceptive acts and practices by Experian
14 were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial
15 injury to consumers that the consumers could not reasonably avoid; this substantial
16 injury outweighed any benefits to consumers or to competition.

17 466. Experian knew or should have known that their computer systems and data
18 security practices were inadequate to safeguard Pennsylvania Subclass members' PII
19 and that risk of a data breach or theft was highly likely. Experian's actions in engaging
20 in the above-named deceptive acts and practices were negligent, knowing and reckless
21 with respect to the rights of members of the Pennsylvania Class.

22 467. Pennsylvania Subclass members seek relief under 73 Pa. Cons. Stat. § 201-
23 9.2, including, but not limited to, injunctive relief, actual damages or \$100 per
24 Pennsylvania Subclass member, whichever is greater, treble damages, and attorneys'
25 fees and costs.

26
27 ///

xxv. South Carolina

COUNT 42

VIOLATION OF THE SOUTH CAROLINA DATA BREACH SECURITY ACT

S.C. Code Ann. § 39-1-90, *et seq.*

(On Behalf of the South Carolina Subclass)

468. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

469. Experian is required to accurately notify Plaintiffs 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).

470. Experian 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).

471. Plaintiffs' and South Carolina Subclass members' PII (e.g., Social Security numbers) includes personal identifying information as covered under S.C. Code Ann. § 39-1-90(D)(3).

472. Because Experian 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), Experian had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by S.C. Code Ann. § 39-1-90(A).

473. As a direct and proximate result of Experian's violations of S.C. Code Ann. § 39-1-90(A), Plaintiffs and South Carolina Subclass members suffered damages, as described above.

1 474. Plaintiffs and South Carolina Subclass members seek relief under S.C.
2 Code Ann. § 39-1-90(G), including, but not limited to, actual damages and injunctive
3 relief.

4 **xxvi. Tennessee**

5 **COUNT 43**

6 **VIOLATION OF THE TENNESSEE PERSONAL CONSUMER INFORMATION**
7 **RELEASE ACT**

8 **Tenn. Code Ann. § 47-18-2107, *et seq.***

9 **(On Behalf of the Tennessee Subclass)**

10 475. Plaintiffs incorporate by reference all paragraphs above as if fully set forth
11 herein.

12 476. Experian is required to accurately notify Plaintiffs and Tennessee Subclass
13 members following discovery or notification of a breach of its data security system (in
14 which unencrypted personal information was, or is reasonably believed to have been,
15 acquired by an unauthorized person) in the most expedient time possible and without
16 unreasonable delay under Tenn. Code Ann. § 47-18-2107(b).

17 477. Experian is a business that owns or licenses computerized data that
18 includes personal information as defined by Tenn. Code Ann. § 47-18-2107(a)(2).

19 478. Plaintiffs' and Tennessee Subclass members' PII (e.g., Social Security
20 numbers) includes personal information as covered under Tenn. Code Ann. § 47-18-
21 2107(a)(3)(A).

22 479. Because Experian discovered a breach of its security system (in which
23 unencrypted personal information was, or is reasonably believed to have been, acquired
24 by an unauthorized person), Experian had an obligation to disclose the data breach in a
25 timely and accurate fashion as mandated by Tenn. Code Ann. § 47-18-2107(b).

26 480. As a direct and proximate result of Experian's violations of Tenn. Code
27 Ann. § 47-18-2107(b), Plaintiffs and Tennessee Subclass members suffered damages, as
28 described above.

1 481. Plaintiffs and Tennessee Subclass members seek relief under Tenn. Code
2 Ann. §§ 47-18-2107(h), 47-18-2104(d), 47-18-2104(f), including, but not limited to,
3 actual damages, injunctive relief and treble damages.

4 **xxvii. Texas**

5 **COUNT 44**

6 **VIOLATION OF THE TEXAS DECEPTIVE TRADE PRACTICES-CONSUMER**
7 **PROTECTION ACT**

8 **Tex. Bus. & Com. Code § 17.46, *et seq.***

9 **(On Behalf of the Tennessee Subclass)**

10 482. Plaintiffs incorporate by reference all paragraphs above as if fully set forth
11 herein.

12 483. By the actions and omission detailed herein, Experian has violated the
13 Texas Deceptive Trade Practices-Consumer Protection Act, Tex. Bus. & Com. Code §
14 17.41, *et seq.* (the “TDTPA”).

15 484. Plaintiffs and members of the Texas Subclass are individuals and, thus,
16 “consumers” as defined in Tex. Bus. & Com. Code § 17.45(4).

17 485. Experian performed “services,” as defined by Tex. Bus. & Com. Code §
18 17.45(2), with respect to its compilation, maintenance, use, and furnishing of Plaintiffs’
19 and Texas Subclass members’ PII that was compromised in the Data Breach.

20 486. Experian engaged in “trade” and “commerce” as defined in Tex. Bus. &
21 Com. Code § 17.45(6), by providing its services to T-Mobile as alleged above, directly
22 or indirectly affecting Texas citizens through that trade and commerce.

23 487. Furthermore, while operating in Texas, Experian engaged in deceptive
24 trade practices in the course of its business and occupation, including by representing
25 that its services had characteristics that they did not have, representing that its services
26 were of a particular standard or quality when they were not, and advertising its services
27 with intent not to sell them as advertised, in violation of Tex. Bus. & Com. Code
28 §17.46(a) and (b). This includes but is not limited to the following:

1 a. Experian failed to enact adequate privacy and security measures to
2 protect the Texas Subclass members' PII from unauthorized disclosure, release, data
3 breaches, and theft, which was a direct and proximate cause of the Data Breach;

4 b. Experian failed to take proper action following known security risks
5 and prior cybersecurity incidents, which was a direct and proximate cause of the Data
6 Breach;

7 c. Experian knowingly and fraudulently misrepresented that it would
8 maintain adequate data privacy and security practices and procedures to safeguard the
9 Texas Subclass members' PII from unauthorized disclosure, release, data breaches, and
10 theft;

11 d. Experian omitted, suppressed, and concealed the material fact of the
12 inadequacy of its privacy and security protections for the Texas Subclass members' PII;

13 e. Experian knowingly and fraudulently misrepresented that it would
14 comply with the requirements of relevant federal and state laws pertaining to the privacy
15 and security of Texas Subclass members' PII, including but not limited to duties
16 imposed by the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801 *et seq.*; and

17 f. Experian failed to maintain the privacy and security of Texas
18 Subclass members' PII, in violation of duties imposed by applicable federal and state
19 laws, including but not limited to those mentioned in the aforementioned paragraph,
20 directly and proximately causing the Data Breach.

21 488. As a direct and proximate result of Experian's practices, Texas Subclass
22 members suffered injury and/or damages, including but not limited to time and expenses
23 related to monitoring their financial accounts for fraudulent activity, an increased,
24 imminent risk of fraud and identity theft, and loss of value of their PII.

25 489. The above unfair and deceptive acts and practices and acts by Experian
26 were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial
27 injury to Texas Subclass members that they could not reasonably avoid; this substantial
28 injury outweighed any benefits to consumers or to competition.

1 490. Experian knew or should have known that its computer systems and data
2 security practices were inadequate to safeguard Texas Subclass members' PII and that
3 risk of a data breach or theft was highly likely. Experian's actions in engaging in the
4 above-named unfair practices and deceptive acts were negligent, knowing and willful.

5 491. Experian engaged in affirmative false and misleading statements,
6 omissions of material fact and deceptive acts, as described in detail herein, upon which
7 Plaintiffs and the Texas Subclass relied upon to their detriment.

8 492. The acts of Experian were a producing cause of the damages suffered by
9 Plaintiffs and the Texas Subclass.

10 493. Specifically, by the facts set forth previously, Experian failed to disclose
11 the inadequate security of its computer systems used to store Plaintiffs' and Texas
12 Subclass members' PII which it knew or should have known were inadequate at the
13 time of the transaction, and Plaintiffs and Texas Subclass members would not have
14 provided their PII to Experian had they known of this information in violation of Tex.
15 Bus. & Com. Code §17.46(b)(24).

16 494. Also specifically, by the facts set forth previously, Experian has made
17 identical, written, false affirmative representations of fact to Plaintiffs and the Texas
18 Subclass as to the adequacy of their privacy protections in violation of Tex. Bus. &
19 Com. Code §17.46(a), (b)(5) and (b)(7), when in fact Experian's systems were
20 inadequate.

21 495. A written pre-suit demand under Tex. Bus. & Com. Code § 17.505(a) is
22 unnecessary and unwarranted because Experian has long had notice of Plaintiffs'
23 allegations, claims and demands, including from the filing of numerous underlying
24 actions against it arising from the Data Breach, the first of which were filed on or about
25 October 2, 2015. Further, Experian is the party with the most knowledge of the
26 underlying facts giving rise to Plaintiffs' allegations, so that any pre-suit notice would
27 not put Experian in a better position to evaluate those claims.
28

1 496. Plaintiffs, individually and on behalf of Texas Subclass members, seek
2 relief under the TDTPA including, but not limited to:

3 a. the amount of economic damages found by the trier of fact as to each
4 Subclass member;

5 b. because Experian committed these violations knowingly and/or
6 intentionally as alleged above, Plaintiffs seek, individually and on behalf of the Texas
7 Subclass, three times the amount of their economic damages under Tex. Bus. & Com.
8 Code §17.50(b)(1);

9 c. an order enjoining such acts or failure to act, any orders necessary to
10 restore to any party to the suit any money or property acquired in violation of this
11 subchapter;

12 d. an award of statutory attorneys' fees and costs; and

13 e. any other relief which the court deems proper, including the
14 appointment of a receiver or the revocation of a license or certificate authorizing a
15 person to engage in business in Texas if the judgment has not been satisfied within three
16 months of the date of the final judgment.

17 **xxviii. Virginia**

18 **COUNT 45**

19 **VIOLATION OF THE VIRGINIA CONSUMER PROTECTION ACT**

20 **Va. Code Ann. § 59.1-196, *et seq.***

21 **(On Behalf of the Virginia Subclass)**

22 497. Plaintiffs incorporate by reference all paragraphs above as if fully set forth
23 herein.

24 498. The Virginia Consumer Protection Act prohibits “[u]sing any . . .
25 deception, fraud, false pretense, false promise, or misrepresentation in connection with a
26 consumer transaction.” Va. Code Ann. § 59.1-200(14).
27
28

1 499. Experian compiled, maintained, used, and furnished Plaintiffs' and
2 Virginia Subclass members' PII in connection with consumer transactions, as defined
3 under Va. Code Ann. § 59.1-198, including for example T-Mobile credit assessments.

4 500. While operating in Virginia, Experian engaged in deceptive trade practices
5 in connection with consumer transactions, including by representing that its services had
6 characteristics that they did not have, representing that its services were of a particular
7 standard or quality when they were not, and advertising its services with intent not to
8 sell them as advertised, in violation of Va. Code Ann. § 59.1-200. This includes but is
9 not limited to the following:

10 a. Experian failed to enact adequate privacy and security measures to
11 protect the Virginia Subclass members' PII from unauthorized disclosure, release, data
12 breaches, and theft, which was a direct and proximate cause of the Data Breach;

13 b. Experian failed to take proper action following known security risks
14 and prior cybersecurity incidents, which was a direct and proximate cause of the Data
15 Breach;

16 c. Experian knowingly and fraudulently misrepresented that it would
17 maintain adequate data privacy and security practices and procedures to safeguard the
18 Virginia Subclass members' PII from unauthorized disclosure, release, data breaches,
19 and theft;

20 d. Experian omitted, suppressed, and concealed the material fact of the
21 inadequacy of its privacy and security protections for the Virginia Subclass members'
22 PII;

23 e. Experian knowingly and fraudulently misrepresented that it would
24 comply with the requirements of relevant federal and state laws pertaining to the privacy
25 and security of Virginia Subclass members' PII, including but not limited to duties
26 imposed by the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801 *et seq.*; and

27 f. Experian failed to maintain the privacy and security of Virginia
28 Subclass members' PII, in violation of duties imposed by applicable federal and state

1 laws, including but not limited to those mentioned in the aforementioned paragraph,
2 directly and proximately causing the Data Breach.

3 501. As a direct and proximate result of Experian's practices, Virginia Subclass
4 members suffered injury and/or damages, including but not limited to time and expenses
5 related to monitoring their financial accounts for fraudulent activity, an increased,
6 imminent risk of fraud and identity theft, and loss of value of their PII.

7 502. The above unfair and deceptive acts and practices and acts by Experian
8 were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial
9 injury to Virginia Subclass members that they could not reasonably avoid; this
10 substantial injury outweighed any benefits to consumers or to competition.

11 503. Experian knew or should have known that its computer systems and data
12 security practices were inadequate to safeguard Virginia Subclass members' PII and that
13 risk of a data breach or theft was highly likely. Experian's actions in engaging in the
14 above-named unfair practices and deceptive acts were negligent, knowing and willful.

15 504. Plaintiffs and Virginia Subclass members seek all available relief under Va.
16 Code Ann. § 59.1-204, including, but not limited to, actual damages; statutory damages
17 and/or penalties in the amount of \$1,000 per violation or, in the alternative, \$500 per
18 violation; restitution, injunctive relief, punitive damages, and attorneys' fees and costs.

19 **COUNT 46**

20 **VIOLATION OF THE VIRGINIA PERSONAL INFORMATION BREACH**
21 **NOTIFICATION ACT**

22 **Va. Code. Ann. § 18.2-186.6, *et seq.***

23 **(On Behalf of the Virginia Subclass)**

24 505. Plaintiffs incorporate by reference all paragraphs above as if fully set forth
25 herein.

26 506. Experian is required to accurately notify Plaintiffs and Virginia Subclass
27 members following discovery or notification of a breach of its data security system (if
28 unencrypted or unredacted personal information was or is reasonably believed to have

1 been accessed and acquired by an unauthorized person who will, or it is reasonably
2 believed who will, engage in identify theft or another fraud) without unreasonable delay
3 under Va. Code Ann. § 18.2-186.6(B).

4 507. Experian is an entity that owns or licenses computerized data that includes
5 personal information as defined by Va. Code Ann. § 18.2-186.6(B).

6 508. Plaintiffs' and Virginia Subclass members' PII (e.g., Social Security
7 numbers) includes personal information as covered under Va. Code Ann. § 18.2-
8 186.6(A).

9 509. Because Experian discovered a breach of their security system (in which
10 unencrypted or unredacted personal information was or is reasonably believed to have
11 been accessed and acquired by an unauthorized person, who will, or it is reasonably
12 believed who will, engage in identify theft or another fraud), Experian had an obligation
13 to disclose the Data Breach in a timely and accurate fashion as mandated by Va. Code
14 Ann. § 18.2-186.6(B).

15 510. As a direct and proximate result of Experian's violations of Va. Code Ann.
16 § 18.2-186.6(B), Plaintiffs and Virginia Subclass members suffered damages, as
17 described above.

18 511. Plaintiffs and Virginia Subclass members seek relief under Va. Code Ann.
19 § 18.2-186.6(I), including, but not limited to, actual damages.

20 **xxix. Washington**

21 **COUNT 47**

22 **VIOLATION OF THE WASHINGTON CONSUMER PROTECTION ACT**

23 **Wash. Rev. Code Ann. § 19.86.020, *et seq.***

24 **(On Behalf of the Washington Subclass)**

25 512. Plaintiffs incorporate by reference all paragraphs above as if fully set forth
26 herein.
27
28

1 513. Experian, while operating in Washington, engaged in unfair and deceptive
2 acts and practices in the conduct of trade or commerce, in violation of Wash. Rev. Code
3 §19.86.020. This includes but is not limited to the following:

4 a. Experian failed to enact adequate privacy and security measures to
5 protect the Washington Subclass members' PII from unauthorized disclosure, release,
6 data breaches, and theft, which was a direct and proximate cause of the Data Breach;

7 b. Experian failed to take proper action following known security risks
8 and prior cybersecurity incidents, which was a direct and proximate cause of the Data
9 Breach;

10 c. Experian knowingly and fraudulently misrepresented that it would
11 maintain adequate data privacy and security practices and procedures to safeguard the
12 Washington Subclass members' PII from unauthorized disclosure, release, data
13 breaches, and theft;

14 d. Experian omitted, suppressed, and concealed the material fact of the
15 inadequacy of its privacy and security protections for the Washington Subclass
16 members' PII;

17 e. Experian knowingly and fraudulently misrepresented that it would
18 comply with the requirements of relevant federal and state laws pertaining to the privacy
19 and security of the Washington Subclass members' PII, including but not limited to
20 duties imposed by the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801 *et*
21 *seq.*;

22 f. Experian failed to maintain the privacy and security of the
23 Washington Subclass members' PII, in violation of duties imposed by applicable federal
24 and state laws, including but not limited to those mentioned in the aforementioned
25 paragraph, directly and proximately causing the Data Breach;

26 g. Experian failed to disclose the Data Breach to the Washington
27 Subclass members in a timely and accurate manner, in violation of the duties imposed
28 by Wash. Rev. Code Ann. § 19.255.010(1).

514. As a direct and proximate result of Experian's practices, the Washington Subclass members suffered injury and/or damages, including but not limited to 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 PII.

515. The above unfair and deceptive acts and practices and acts by Experian were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to the Washington Subclass members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

516. Experian knew or should have known that its computer systems and data security practices were inadequate to safeguard the Washington Subclass members' PII and that risk of a data breach or theft was highly likely. Experian's actions in engaging in the above-described unfair practices and deceptive acts were negligent, knowing and willful.

517. Plaintiffs and the Washington Subclass members seek relief Wash. Rev. Code § 19.86.090, including but not limited to actual damages (to be proven at trial), treble damages, injunctive relief, and attorneys' fees and costs.

COUNT 48

VIOLATION OF THE WASHINGTON DATA BREACH NOTICE ACT

Wash. Rev. Code Ann. § 19.255.010, *et seq.*

(On Behalf of the Washington Subclass)

518. Plaintiffs incorporate by reference all paragraphs above as if fully set forth herein.

519. Under Wash. Rev. Code Ann. § 19.255.010(1), “[a]ny person or business that conducts business in this state and that owns or licenses data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person”

1 520. Under Wash. Rev. Code Ann. § 19.255.010(2), “[a]ny person or business
2 that maintains data that includes personal information that the person or business does
3 not own shall notify the owner or licensee of the information of any breach of the
4 security of the data immediately following discovery, if the personal information was,
5 or is reasonably believed to have been, acquired by an unauthorized person.”

6 521. Under Wash. Rev. Code Ann. § 19.255.010 (16), “[n]otification to affected
7 consumers ... under this section must be made in the most expedient time possible and
8 without unreasonable delay, no more than forty-five calendar days after the breach was
9 discovered.”

10 522. The Experian Defendants are businesses that conduct business in
11 Washington that own or license computerized data that includes personal information,
12 as defined by Wash. Rev. Code Ann. § 19.255.010.

13 523. Plaintiffs and the Washington Subclass members’ PII (including but not
14 limited to names, addresses, and social security numbers) includes personal information
15 covered under Wash. Rev. Code Ann. § 19.255.010(5).

16 524. Because Experian discovered a breach of its security system in which
17 personal information was, or is reasonably believed to have been, acquired by an
18 unauthorized person and the personal information was not secured, Experian had an
19 obligation to disclose the Data Breach in a timely and accurate fashion as mandated
20 under Wash. Rev. Code Ann. § 19.255.010(16).

21 525. By failing to disclose the Data Breach in a timely and accurate manner,
22 Experian violated Wash. Rev. Code Ann. § 19.255.010(16).

23 526. As a direct and proximate result of Experian’s violations of Wash. Rev.
24 Code Ann. § 19.255.010(16), Plaintiffs and the Washington Subclass members suffered
25 the damages described above.

26 527. Plaintiffs and the Washington Subclass members seek relief under Wash.
27 Rev. Code Ann. §§ 19.255.010(13)(a), (b) including but not limited to actual damages
28 (to be proven at trial) and injunctive relief.

RELIEF REQUESTED

Plaintiffs, on behalf of themselves and all others similarly situated, request that the Court enter judgment against Experian as follows:

- A. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Nationwide Class and Statewide Subclasses as requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class and Statewide Subclasses requested herein;
- B. Injunctive relief requiring Defendants to (1) strengthen their data security systems that maintain PII to comply with the FCRA and GLBA, the applicable state laws alleged herein (including but not limited to the California Customer Records Act) and best practices under industry standards; (2) engage third-party auditors and internal personnel to conduct security testing and audits on Defendants' systems on a periodic basis; (3) promptly correct any problems or issues detected by such audits and testing; and (4) routinely and continually conduct training to inform internal security personnel how to prevent, identify and contain a breach, and how to appropriately respond;
- C. An order requiring Defendants to pay all costs associated with Class notice and administration of Class-wide relief;
- D. An award to Plaintiffs and all Class (and Subclass) Members of compensatory, consequential, incidental, and statutory damages, restitution, and disgorgement, in an amount to be determined at trial;
- E. An award to Plaintiffs and all Class (and Subclass) Members of additional credit monitoring and identity theft protection services beyond the two-year package Experian is currently offering;
- F. An award of attorneys' fees, costs, and expenses, as provided by law or equity;

G. An order Requiring Defendants to pay pre-judgment and post-judgment interest, as provided by law or equity; and

F. Such other or further relief as the Court may allow.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of all issues in this action so triable of right.

Dated: April 15, 2016

Respectfully submitted,

AHDOOT & WOLFSON, PC

/s/ Tina Wolfson
Tina Wolfson
twolfson@ahdootwolfson.com
1016 Palm Avenue
West Hollywood, CA 90069
Telephone: 310-474-911
Fax: 310-474-8585

Daniel S. Robinson
drobinson@rcrsd.com
**ROBINSON CALCAGNIE ROBINSON
SHAPIRO DAVIS, INC.**
19 Corporate Plaza Dr.
Newport Beach, CA 92660
Telephone: (949) 720-1288

Plaintiffs' Interim Co-Lead Counsel

BERGER & MONTAGUE, P.C.

Sherrie Savett
Shanon Carson
Jon Lambiras
1622 Locust St.
Philadelphia, PA 19103
Telephone: (215) 875-3000
Fax: (215) 875-4604
ssavett@bm.net
scarson@bm.net
jlambiras@bm.net

Daniel C. Girard (State Bar No. 114826)

1 Scott M. Grzenczyk (State Bar No. 279309)
2 Linh G. Vuong (State Bar No. 286837)

Girard Gibbs LLP

601 California Street, 14th Floor

San Francisco, CA 94108

Tel: (415) 981-4800

Fax: (415) 981-4846

dgc@girardgibbs.com

smg@girardgibbs.com

lgv@girardgibbs.com

7 Cari Campen Laufenberg, *admitted pro hac vice*
8 claufenberg@kellerrohrback.com

9 Gretchen Freeman Cappio, *pro hac vice*
10 *forthcoming*

gcappio@kellerrohrback.com

11 Amy N. L. Hanson, *admitted pro hac vice*

ahanson@kellerrohrback.com

KELLER ROHRBACK L.L.P.

12 1201 Third Avenue, Suite 3200

13 Seattle, Washington 98101-3052

14 Telephone: (206) 623-1900

Fax: (206) 623-3384

15 Matthew J. Preusch, CA Bar No. 298144

16 mpreusch@kellerrohrback.com

KELLER ROHRBACK L.L.P.

17 1129 State Street, Suite 8

18 Santa Barbara, California 93101

19 Telephone: (805) 456-1496

Fax: (805) 456-1497

20 Christopher P. Ridout, (CA Bar No. 143931)

ZIMMERMAN REED, LLP

21 2381 Rosecrans Avenue, Suite 328

22 Manhattan Beach, CA 90245

23 Telephone: (877) 500-8780

Facsimile: (888) 490-7750

24 christopher.ridout@zimmreed.com

25 David M. Cialkowski, (MN Bar No. 306526)

26 Brian C. Gudmundson (MN Bar No. 336695)

ZIMMERMAN REED, LLP

27 1100 IDS Center, 80 South 8th St.

28 Minneapolis, MN 55402

Telephone: (612) 341-0400

Facsimile: (612) 341-0844
david.cialkowski@zimmreed.com
brian.gudmundson@zimmreed.com

Michael A. Galpern (*pro hac vice*)
Andrew P. Bell (*pro hac vice*)
James A. Barry (*pro hac vice*)
LOCKS LAW FIRM, LLC
801 N. Kings Highway
Cherry Hill, NJ 08034
Tel: (856) 663-8200
Fax: (856) 661-8400

Joseph N. Kravec, Jr.
JKravec@fdpklaw.com
**FEINSTEIN DOYLE PAYNE & KRAVEC,
LLC**
Allegheny Building, 17th Floor
429 Forbes Avenue
Pittsburgh, PA 15219
1-412-281-8400
1-412-281-1007 (FAX)

Plaintiffs' Steering Committee