

1 Matthew J. Preusch (SBN 298144)  
2 mpreusch@kellerrohrback.com  
3 **KELLER ROHRBACK L.L.P.**  
4 1129 State Street, Suite 8  
5 Santa Barbara, CA 93101  
6 T: (805) 456-1496  
7 F: (805) 456-1497

8 Lynn Lincoln Sarko, *admitted pro hac vice*  
9 lsarko@kellerrohrback.com  
10 **KELLER ROHRBACK L.L.P.**  
11 1201 Third Avenue, Suite 3200  
12 Seattle, WA 98101  
13 T: (206) 623-1900  
14 F: (206) 623-3384  
15 *Attorneys for Plaintiffs Michael Corona and*  
16 *Christina Mathis*

17 Daniel C. Girard (SBN 114826)  
18 dcg@girardgibbs.com  
19 **GIRARD GIBBS LLP**  
20 601 California Street, 14th Floor  
21 San Francisco, CA 94108  
22 T: (415) 981-4800  
23 F: (415) 981-4846  
24 *Attorneys for Plaintiffs Joshua Forster and*  
25 *Ella Carline Archibeque*

Michael W. Sobol (SBN 194857)  
msobol@lchb.com  
**LIEFF CABRASER HEIMANN &  
BERNSTEIN, LLP**  
275 Battery Street, 29th Floor  
San Francisco, CA 94111-3339  
T: (415) 956-1000  
F: (415) 956-1008  
*Attorneys for Plaintiffs Michael  
Levine and Geoffrey Springer*

26 *Additional Counsel listed below*

27 **UNITED STATES DISTRICT COURT**  
28 **CENTRAL DISTRICT OF CALIFORNIA**

29 MICHAEL CORONA, CHRISTINA  
30 MATHIS, et al., individually and on  
31 behalf of others similarly situated,

32 Plaintiffs,

33 vs.

34 SONY PICTURES ENTERTAINMENT,  
35 INC.,

36 Defendant.

**CASE NO. 2:14-CV-09600-RGK-SH**

**CLASS ACTION**

**AMENDED CLASS ACTION  
COMPLAINT**

**JURY TRIAL DEMANDED**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Raúl Pérez  
Raul.Perez@Capstonelawyers.com  
**CAPSTONE LAW APC**  
1840 Century Park East, Suite 450  
Los Angeles, CA 90067  
T: (310) 556-4811  
F: (310) 943-0396  
*Attorneys for Plaintiff Marcela Bailey*

Steven M. Tindall  
stindall@rhdtlaw.com  
**RUKIN HYLAND DORIA &  
TINDALL LLP**  
100 Pine Street, Suite 2150  
San Francisco, CA 94111  
T: (415) 421-1800  
F: (415) 421-1700

John H. Gomez  
john@gomeztrialattorneys.com  
**GOMEZ TRIAL ATTORNEYS**  
655 West Broadway, Suite 1700  
San Diego, CA 92101  
T: (619) 237-3490  
F: (619) 237-3496  
*Attorneys for Plaintiffs Steven Shapiro  
and Lawon Exum*

**TABLE OF CONTENTS**

	<u>Page</u>
I. INTRODUCTION .....	1
II. NATURE OF THE ACTION .....	1
III. JURISDICTION .....	4
IV. PARTIES .....	5
V. FACTUAL ALLEGATIONS .....	6
A. The Data Breach Exposed the Financial, Medical and Other Personal Information of SPE’s Current and Former Employees .....	6
B. Successive Data Breaches at SPE and Other Sony Companies Exposed Data Security Weaknesses .....	11
C. Ignoring Prior Data Breaches and the Warnings of Its Employees and Third-Party Auditors, SPE Favored Cost Savings and Convenience Over Sound Data Security Principles .....	14
D. Current and Former SPE Employees Are Victims of the Breach.....	22
VI. PLAINTIFFS’ MOST SENSITIVE INFORMATION IS BREACHED, CAUSING LIFELONG DATA INSECURITY .....	29
A. Michael Corona .....	29
B. Christina Mathis .....	32
C. Joshua Forster.....	35
D. Ella Carline Archibeque .....	38
E. Michael Levine.....	41
F. Geoffrey Springer.....	43
G. Marcela Bailey .....	46

1	H. Steven Shapiro.....	49
2	I. Lawon Exum .....	52
3	VII. CLASS ACTION ALLEGATIONS .....	54
4	VIII. CAUSES OF ACTION.....	58
5	IX. PRAYER FOR RELIEF .....	95
6	X. JURY TRIAL DEMANDED.....	95
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**I. INTRODUCTION**

Plaintiffs Michael Corona, Christina Mathis, Joshua Forster, Ella Carline Archibeque, Michael Levine, Geoffrey Springer, Marcela Bailey, Steven Shapiro, and Lawon Exum (“Plaintiffs”), individually and on behalf of all others similarly situated, file this Amended Class Action Complaint against Sony Pictures Entertainment, Inc. (“Defendant” or “SPE”), and allege as follows based on personal knowledge, the investigation of their counsel, and information and belief.

**II. NATURE OF THE ACTION**

1. An epic nightmare, much better suited to a cinematic thriller than to real life, has been unfolding in slow motion for thousands of current and former employees of SPE. In late November and December 2014, they learned that they were the victims of a massive data breach first publicized by the media in late November 2014 (the “Data Breach”) that resulted in the posting of SPE’s personnel records on the internet. The Data Breach resulted in the public disclosure of employees’ most sensitive, non-public personal identifying information (“PII”), including Social Security numbers, employment files, salary and bank account information, health insurance and other medical information, their names, home and email addresses, visa and passport numbers, and retirement plan data, as well as their family members’ similar information. These records were and are posted on file-sharing websites for identity thieves to download, have been published in news

1 reports, and were used to send emails threatening physical harm to employees and  
2 their families.<sup>1</sup>  
3

4 2. Cybercriminals were able to perpetrate a breach of this depth and scope  
5 because SPE failed to maintain reasonable and adequate security measures to protect  
6 the employees' information from access and disclosure. SPE has obligations, by  
7 statute and otherwise, to protect its employees' employment and personnel records  
8 from unauthorized access, yet failed at numerous opportunities to prevent, detect,  
9 end, or limit the scope of the breach. Among other things, (1) SPE failed to  
10 implement security measures designed to prevent this attack even though there have  
11 been similar cyber-attacks of SPE and its sister companies; (2) SPE failed to employ  
12 security protocols to detect the breach and removal of nearly 100 terabytes of data  
13 from its computer networks; and (3) SPE failed to maintain basic security measures  
14 such as access controls and requiring passwords with appropriate levels of  
15 complexity and encryption, measures that would have ensured that data would be  
16  
17  
18  
19  
20  
21

---

22 <sup>1</sup> As Plaintiffs have represented to the Court, simultaneously with the filing of this  
23 Amended Class Action Complaint, Plaintiffs in the following actions are filing  
24 notices of voluntary dismissal without prejudice filed under Fed. R. Civ. P. 41, and  
25 will proceed as named plaintiffs or proposed class members in this action:

- 26 • *Forster et al. v. Sony Pictures Entertainment, Inc.*, No. 2:14-cv-09646-RGK-SH  
27 • *Levine et al. v. Sony Pictures Entertainment, Inc.*, No. 2:14-cv-09687-RGK-SH  
28 • *Bailey v. Sony Pictures Entertainment, Inc.*, No. 2:14-cv-09755-RGK-SH  
• *Shapiro v. Sony Pictures Entertainment, Inc.*, No. 2:14-cv-09762-RGK-SH  
• *Rodriguez v. Sony Pictures Entertainment, Inc.*, No. 2:15-cv-00014-RGK-SH  
• *Exum v. Sony Pictures Entertainment, Inc.*, No. 2:15-cv-00111-CAS-RGK-SH

1 harder to access or steal and, in the event data were accessed or stolen, it would be  
2 unreadable and thus cause less damage to SPE employees and their families.

3  
4 3. Following the breach, SPE has focused on its own remediation efforts,  
5 *not* on protecting its employees' sensitive records or minimizing the harm to its  
6 employees and their families. Rather, SPE has focused on securing its own  
7 intellectual property from pirates and a public relations campaign directed at  
8 controlling the damage to SPE associated with the release of embarrassing internal  
9 emails. Meanwhile, SPE delayed confirming the Data Breach and left its employees  
10 in the dark about the scope of the breach, how they and their families were impacted,  
11 and what steps SPE is taking to remedy or mitigate the breach. Due to SPE's delay,  
12 current and former SPE employees have purchased identity protection services and  
13 insurance and taken other measures to protect their compromised PII, yet remain  
14 vulnerable to identity theft, medical identity theft, tax fraud, and financial theft  
15 because their Social Security numbers, financial information and medical information  
16 have been, and may still be, publicly available to anyone with an internet connection.  
17 SPE's conduct is a direct cause of the ongoing harm employees are currently  
18 suffering and will continue to experience for the indefinite future.

19  
20  
21  
22  
23  
24 4. Plaintiffs are former SPE employees who bring this proposed class  
25 action lawsuit on behalf of employees whose PII has been compromised as a result of  
26 the Data Breach. Plaintiffs and class members, as well as their family members, will  
27 have to remain vigilant for the rest of their lives to combat potential identity theft  
28

1 arising from the staggering amount of financial, medical and other personal  
2 information that is not only in the hands of cyber criminals, but that has also been  
3  
4 posted on the internet for anyone to gather and use for any purpose, at any time, in  
5 perpetuity. Despite all best efforts of Plaintiffs, class members, or anyone else, this  
6 most sensitive personal data can never be made private again.  
7

8 5. Plaintiffs allege that SPE failed to adequately safeguard its current and  
9 former employees' PII, including Social Security numbers, medical records, and  
10 financial information, in compliance with applicable law. Plaintiffs seek injunctive  
11 relief requiring SPE to implement and maintain security practices to comply with  
12 regulations designed to prevent and remedy these types of breaches, as well as  
13 restitution, damages, and other relief.  
14  
15

### 16 III. JURISDICTION

17 6. This Court has jurisdiction over this action pursuant to 28 U.S.C.  
18 § 1332(d) because the amount in controversy exceeds \$5 million, exclusive of interest  
19 and costs, and members of the proposed class are citizens of different states than  
20 Defendant SPE.  
21

22 7. This Court has personal jurisdiction over SPE because SPE maintains its  
23 headquarters in California, is registered to conduct business in California, and has  
24 sufficient minimum contacts with California.  
25  
26  
27  
28



1 8. Venue is proper in this district under 28 U.S.C. § 1391(b) because SPE  
2 resides in this district and a substantial part of the events or omissions giving rise to  
3 Plaintiffs' claims occurred in this district.  
4

5 **IV. PARTIES**

6 9. Plaintiff Michael Corona is a resident of Virginia.

7  
8 10. Plaintiff Christina Mathis is a resident of California

9 11. Plaintiff Joshua Forster is a resident of Colorado.

10 12. Plaintiff Ella Carline Archibeque is a resident of California.

11  
12 13. Plaintiff Michael Levine is a resident of California.

13 14. Plaintiff Geoffrey Springer is a resident of Virginia.

14  
15 15. Plaintiff Marcela Bailey is a resident of California.

16 16. Plaintiff Steven Shapiro is a resident of California.

17 17. Plaintiff Lawon Exum is a resident of California.

18 18. Each Plaintiff had sensitive, non-public information compromised due to  
19 the Data Breach and has been injured as a result.  
20

21 19. Defendant Sony Pictures Entertainment, Inc. is a corporation organized  
22 under the laws of Delaware with its principal place of business in Culver City,  
23 California.  
24

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

## V. FACTUAL ALLEGATIONS

### A. The Data Breach Exposed the Financial, Medical and Other Personal Information of SPE's Current and Former Employees

20. On November 24, 2014, the media reported that SPE was subject to an undetected data breach whereby nearly 100 terabytes of data was seized from the company and caused the leak of the financial, medical, and other personal information of thousands of current and former employees on the internet.

21. A hacker group calling itself the Guardians of Peace, or “#GOP”, took over SPE's network, displayed its own messages and an image of a skeleton, seized control of promotional Twitter accounts for SPE movies, and warned SPE that it had obtained “secrets” that it threatened to leak on the Web:



22. The hackers began releasing portions of stolen data to the public on November 30, 2014, beginning with a series of unreleased movies produced by SPE. The media then reported receiving emails with links to a file on Pastebin, a file-sharing site that contained a trove of SPE employees' personnel information.

1           23. Security researcher Brian Krebs, who was the first to uncover many of  
2 the recent high-profile data breaches at companies like Target Corporation and The  
3 Home Depot, reported in a December 2, 2014 blog post that several of his sources  
4 had confirmed that the hackers had stolen more than 25 gigabytes of sensitive data,  
5 including Social Security numbers and medical and salary information, of tens of  
6 thousands of current and former SPE employees.  
7

9           24. Mr. Krebs reported that he had observed files being traded on torrent  
10 networks, including a global employee list containing names, employee IDs,  
11 usernames, and birthdates of current and former SPE employees, and a list containing  
12 names, birthdates, Social Security numbers and health savings account data. The  
13 files included a Microsoft Excel document with the name, location, employee ID,  
14 network username, base salary and date of birth of more than 6,800 employees; a  
15 status report from April 2014 listing the names, dates of birth, Social Security  
16 numbers and health savings account data of more than 700 employees; and a file that  
17 appeared to be part of an internal audit report from PricewaterhouseCoopers, made up  
18 of screen shots of dozens of employees' federal tax records and other compensation  
19 data. Mr. Krebs found that a "comprehensive search on LinkedIn for dozens of  
20 names in the [Microsoft Excel] list indicate[d] that virtually all correspond to current  
21 or former Sony employees."  
22

23  
24           25. Kevin Roose, a well-regarded technology writer, reported that the initial  
25 leak also included a spreadsheet listing the names, birth dates, and Social Security  
26  
27  
28

1 numbers of 3,803 SPE employees; a spreadsheet listing the division-by-division SPE  
2 payroll, as well as costs for raises and other pay changes; a spreadsheet listing SPE  
3 employees who were fired or laid off in 2014 as part of the company's  
4 reorganization, along with the reasons for their terminations and the estimated costs  
5 for severance pay, COBRA health benefits, and outplacement costs; and detailed  
6 performance reviews for hundreds of SPE employees.  
7  
8

9         26. On December 5, 2014, sources reported that the Data Breach had  
10 exposed even more personal information than had been previously reported,  
11 including over 47,000 unique Social Security numbers, more than 15,200 of which  
12 belong to current and former SPE employees. Some of these employees were last  
13 employed by SPE as long ago as 1955, raising concerns about SPE's data retention  
14 policies. The Social Security numbers were copied more than 1.1 million times  
15 throughout the 601 files stolen by hackers according to Identity Finder LLC, which  
16 analyzed the breached data. This personal information was found in more than 500  
17 spreadsheets, 75 PDFs, and several Microsoft Word documents, none of which were  
18 protected by passwords. As Identity Finder CEO Todd Feinman explained, personal  
19 information such as Social Security numbers should be stored in one place with  
20 password protection and "[l]eaving these files open is not making the hackers' job  
21 difficult." The files have since been posted online on multiple file-sharing websites.  
22  
23  
24  
25  
26

27         27. Hackers also used the stolen data to threaten SPE's employees and their  
28 families with physical harm. On December 5, 2014, many current and former SPE

1 employees received an email in which they were told: “[p]lease sign your name to  
2 object the false [sic] of the company at the email address below if you don’t want to  
3 suffer damage. If you don’t, not only you but your family will be in danger.”

4  
5 28. As of December 8, 2014, hackers had released around 140 gigabytes of a  
6 cache of internal SPE files and films they claimed totals around 100 terabytes—  
7 approximately ten times the amount of information stored in the Library of Congress.  
8 Two days later, the hackers posted additional data with a message to SPE employees  
9 threatening to release even more of their sensitive personal information:  
10

11  
12 SPE Employees!

13 Don’t believe what the executives of SPE says.

14 They say as if the FBI could resolve everything.

15  
16 But the FBI cannot find us because we know everything about what’s  
17 going on inside the FBI.

18 We still have huge amount of sensitive information to be released  
19 including your personal details and mailboxes.

20 If continued wrongdoings of the executives of SPE drive us to make an  
21 unwanted decision, only SPE should be blamed.

22 Now is the time for you to choose what to do.

23 We have already given much time for you.

24  
25 29. The hackers posted an estimated 38 million files on file-sharing sites in  
26 eight separate leaks, consisting of massive amounts of SPE employee data in addition  
27 to internal SPE emails, profit-and-loss statements, and scripts for upcoming SPE  
28 television shows and movies. The leaked employee data included names, employee

1 IDs, dates of birth, home addresses, Social Security numbers, copies of passports and  
2 visas, job titles, salaries and bonus information, tax records, employment contracts,  
3  
4 information regarding employee benefits, medical plans, dental plans, workers  
5 compensation details, retirement and termination plans, receipts for travel, prior work  
6 history, performance reviews, criminal background checks, and details of severance  
7 packages.  
8

9         30. The leaks also included SPE employees' medical information, and the  
10 medical information of their family members. For example, one memo from a human  
11 resources executive to the company's benefits committee disclosed details of an  
12 employee's child with special needs, including the child's name, diagnosis and details  
13 of the child's treatment. The leaked data also includes emails between SPE's  
14 insurance company and its human resources department about the surgery of a named  
15 employee's spouse and another employee's claim for speech therapy lessons.  
16  
17 Another leaked document was a spreadsheet from a human resources folder that  
18 includes the birth dates, gender, health condition, and medical costs for 34 SPE  
19 employees, their spouses and children. The listed conditions include premature  
20 births, cancer, kidney failure and alcoholic liver cirrhosis, though not the employees'  
21 names. Even without the names, however, the document's inclusion of "member  
22 keys" and birth dates could allow someone with access to other employee documents  
23 to identify the employees. Another leaked document listed the Social Security  
24 numbers, insurance policy numbers, names, birth dates and addresses for more than  
25  
26  
27  
28

1 100 employees. Several other leaked documents detailing overpayments made by  
2 Aetna contained insurance claim numbers, member identification numbers, and the  
3 names of employees.  
4

5 **B. Successive Data Breaches at SPE<sup>2</sup> and Other Sony Companies Exposed**  
6 **Data Security Weaknesses**

7 31. SPE has been a longstanding and frequent target for hackers, but it  
8 apparently made a conscious and deliberate business decision to accept both the risk  
9 of losses and the actual losses associated with being hacked.  
10

11 32. SPE's sister companies, Sony Network Entertainment International LLC  
12 and Sony Computer Entertainment America LLC, experienced massive data breaches  
13 in April 2011, which compromised information from approximately 101 million users  
14 accounts, including 12 million unencrypted credit card numbers. Two weeks before  
15 those breaches, the companies received an anonymous warning:  
16

17  
18 You have abused the judicial system in an attempt to censor information  
19 on how your products work . . . Now you will experience the wrath of  
20 Anonymous. You saw a hornet's nest and stuck your [expletive] in it.  
21 You must face the consequences of your actions, Anonymous style. . .  
22 Expect us.

23 33. One of the 2011 data breaches involved Sony's PlayStation® Network  
24 ("PSN"). After the data breach became public, it became clear that while the Sony  
25 companies invested significant resources in protecting their own confidential  
26

---

27  
28 <sup>2</sup> SPE is an indirect, wholly owned subsidiary of Sony Corporation of America  
("Sony America"), which is a wholly owned, indirect subsidiary of Sony  
Corporation ("Sony").

1 proprietary information, they failed to establish even the most basic safeguards for  
2 the PSN and its consumer data. Among other things, the PSN was not protected by  
3 appropriate firewalls, a deviation from widespread industry practice and standards.  
4 As a result, hackers were able to steal the personal information associated with all of  
5 the approximately 77 million customer accounts. Experts have attributed the PSN  
6 breach to an unsophisticated method of hacking that would not have been successful  
7 if even the most basic security measures had been in place.  
8  
9

10 34. PSN users filed class action cases after the 2011 breach, which Sony  
11 agreed to settle in June 2014 in exchange for \$15 million in games, online currency,  
12 and identity theft reimbursement.  
13

14 35. Following the PSN breach, Shinji Hasejima, Chief Information Officer  
15 of SPE's parent Sony, admitted that the attack exploited a "known vulnerability" in  
16 the application server platform used in the PSN. Sony President Kazuo Hirai  
17 admitted that the company's security had been inadequate before the attack, saying  
18 that after the hack, the company had "basically ... done everything to bring our  
19 practices at least in line with industry standards or better."  
20  
21

22 36. Despite these public statements that the company had corrected its  
23 inadequate security measures, Sony's networks remained highly vulnerable to attack.  
24 John Bumgarner, the chief technology officer of the United States Cyber-  
25 Consequences Unit, uncovered numerous security problems on company webpages  
26  
27  
28



1 that were readily accessible. He discovered that unauthorized users could still access  
2 internal Sony resources, including security management tools.

3  
4 37. In June 2011, SPE itself experienced a data breach in which hackers  
5 stole the personal data of over one million customers and released more than 150,000  
6 of the stolen records. The stolen data included names, home addresses, birthdates,  
7 email addresses, and phone numbers, as well as customer passwords, which were  
8 stored unencrypted.

9  
10 38. Following the 2011 data breaches, PCWorld technology journalist Tony  
11 Bradley observed that Sony “seems to ignore compliance requirements and basic  
12 security best practices, so it is basically begging to be attacked.” He advised  
13 companies to follow security “best practices and data security compliance  
14 requirements”—and in short—“Don’t be a Sony.” Fred Touchette of email and web  
15 security firm AppRiver echoed Bradley’s comments, saying, “There is no doubt that  
16 Sony needs to spend some major effort in tightening up its network security. This  
17 latest hack against them was a series of simple SQL Injection attacks against its web  
18 servers. This simply should not have happened.”

19  
20 39. Sony’s security gaps, and the attacks, continued. In 2013, hackers  
21 infiltrated Sony’s network, stole gigabytes of data several times a week and encrypted  
22 the information to cover their tracks.

23  
24 40. In February 2014, hackers accessed an FTP server used in connection  
25 with SPE’s international theatrical sales and distribution system, SpiritWorld. The  
26  
27  
28

1 login credentials for two user accounts were compromised and the personal data of  
2 759 individuals associated with theaters in Brazil, along with payment information  
3 for Brazil film distributors, was stolen. SPE had been storing the payment  
4 information as .txt files since 2008.  
5

6 41. In August 2014, approximately one month after Sony settled the class  
7 action litigation brought by PlayStation® gamers as a result of the April 2011  
8 breach—and just three months before the Data Breach at SPE—hackers again took  
9 down the PSN as well as the Sony Entertainment Network via “denial of service”  
10 attacks. The hackers posted on Twitter that their attacks were intended to raise  
11 awareness of Sony’s inadequate security measures.  
12  
13

14 **C. Ignoring Prior Data Breaches and the Warnings of Its Employees and**  
15 **Third-Party Auditors, SPE Favored Cost Savings and Convenience Over**  
16 **Sound Data Security Principles**

17 42. Given the recent increase of data breaches aimed at major corporations  
18 and the prior data breaches at SPE and its sister companies, one would expect that  
19 SPE would be more vigilant than ever regarding the need to adopt, implement, and  
20 maintain security measures to protect its confidential data, including its employees’  
21 PII. Instead, SPE has emphasized cost savings over compliance when it comes to  
22 data security.  
23  
24

25 43. The technology and business website CIO reported that a 2005 audit of  
26 SPE’s security practices alerted Jason Spaltro, SPE’s executive director of  
27 information security, to several security weaknesses in the company’s systems,  
28

1 including insufficiently strong access controls, a key Sarbanes-Oxley requirement. In  
2 a 2007 interview, Mr. Spaltro was interviewed about compliance with security and  
3 privacy regulations. Discussing the risk analysis of protecting private data, he  
4 weighed the hypothetical \$10 million cost of preventing a potential intrusion against  
5 the hypothetical \$1 million cost of responding to a breach. “With those numbers,  
6 says Spaltro, ‘it’s a valid business decision to accept the risk’ of a security breach. ‘I  
7 will not invest \$10 million to avoid a possible \$1 million loss,’ he suggests.”

10 44. Ari Schwartz, a privacy expert at the Center for Democracy and  
11 Technology, called Spaltro’s reasoning “shortsighted” because the cost of notification  
12 is only a small part of the potential cost to a company. Indeed, Sony reported that the  
13 2011 PSN data breach cost the company \$170 million.

16 45. On information and belief, in 2011, SPE tasked a group of employees to  
17 conduct an assessment of the company’s data security practices. The assessment was  
18 designed to: (1) identify vulnerable data—referred to as “IT assets”—that would be  
19 embarrassing if compromised and made publicly available; (2) identify existing  
20 security gaps with regard to protecting the implicated IT assets; and (3) recommend  
21 steps that could be taken to eliminate these security gaps.

24 46. The project was conducted over two months in 2011, and one of the  
25 principal IT assets identified by the group was a series of databases containing  
26 employee PII. Specifically, the group found that human resources records containing  
27 employees’ PII were unencrypted (“cleartext”) and were universally accessible on  
28

1 SPE's network. The group recommended, among other things, that the identified  
2 databases be both encrypted and segregated from the rest of SPE's network (with  
3 access being as limited as possible). These recommendations—as well as the  
4 identification of the databases and their vulnerabilities—were incorporated into a  
5 final report, which took the form of a PowerPoint presentation sent to Mr. Spaltro and  
6 SPE CIO Steven Andajar. SPE declined to adopt its own security recommendations,  
7 as evidenced by the fact that employee PII was stolen, in unencrypted form, in the  
8 Data Breach.  
9

10  
11  
12 47. Nevertheless, Lockheed Martin security researchers notably publicized  
13 in March 2011 a cyberattack kill chain process, which was developed as a response to  
14 a new, sophisticated type of hacking called advanced persistent threats (“APTs”) that  
15 were bypassing traditional static cyber security tools and allowing information  
16 security professionals to proactively remediate and mitigate targeted, coordinated,  
17 purposeful, and persistent future cyber threats. The kill chain takes advantage of the  
18 seven steps a hacker must take to plan and execute a successful attack and allows  
19 companies to thwart the APT cyberattack by stopping the hacker from completing  
20 *just one* of these seven required steps. In other words, a company has several  
21 different opportunities along the kill chain to thwart an attack.  
22

23  
24  
25 48. In 2013, reports from the United States government and several private  
26 security research firms widely distributed reports about new types of malicious  
27  
28

1 computer code that should have put SPE on notice that cyber-attacks on retailers  
2 continued to evolve.

3  
4 49. Nevertheless, SPE's security practices continued to fall below not only  
5 prudent industry standards for prevention, detection, and/or containment of APT  
6 hacking, but also traditional, static cyber-attack security standards.

7  
8 50. On information and belief, between 2013 and 2014, a project was  
9 undertaken to migrate 10 million SPE documents from one database called Stellent to  
10 another called Al Fresco. The migration included payroll information and other  
11 sensitive PII. None of the data in the Stellent database was encrypted. And less than  
12 one third of the data was encrypted after it was migrated to Al Fresco. SPE  
13 deliberately chose to leave the data unencrypted for the sake of convenience  
14 (encrypted information is not searchable), despite the risks it posed to the security of  
15 important and sensitive PII.

16  
17  
18 51. SPE's security practices continue to fall below prudent industry  
19 standards. Kevin Roose reported that SPE took a "remarkably lax approach to data  
20 security," given that some of the files released in the Data Breach that contained  
21 personal employee data were "unencrypted Excel and Word files, labeled plain as  
22 day." Time Magazine reported a former employee's criticism of SPE's information  
23 security team and that SPE largely ignored the employees' reports of security  
24 violations: "Sony's 'information security' team is a complete joke. We'd report  
25 security violations to them and our repeated reports were ignored." SPE also  
26  
27  
28

1 dedicated insufficient resources to data security. The leaked documents show that out  
2 of 7,000 employees, only eleven were assigned to the information security team, far  
3 too few for a multi-billion dollar company with vast amounts of confidential data.  
4

5 52. Just two months before the Data Breach became public, on September  
6 25, 2014, PricewaterhouseCoopers delivered a report of its audit of SPE's computer  
7 network. The report detailed gaps in the company's monitoring of its systems,  
8 including a firewall and more than 100 other devices that were not being monitored  
9 by the corporate security team in charge of overseeing infrastructure. The auditors  
10 found that SPE had failed to notify the corporate security team of newly added  
11 devices to monitor, including web servers and routers. PricewaterhouseCoopers  
12 warned that "[s]ecurity incidents impacting these network or infrastructure devices  
13 may not be detected or resolved timely." The report concluded that SPE "was failing  
14 to monitor 149 out of a final total of 869 systems they wished to monitor. That meant  
15 they were blind to 17 percent of their environment."  
16  
17  
18  
19

20 53. The leaked emails also exposed lax security practices, including CEO  
21 Michael Lynton "routinely receiv[ing] copies of his passwords in unsecure emails for  
22 his and his family's mail, banking, travel and shopping accounts, from his executive  
23 assistant, David Diamond." A leaked email from October 2014 reveals additional  
24 problems with SPE's computer system. David C. Hendler, SPE's CFO, complained  
25 that the company had experienced months of "significant and repeated outages due to  
26 a lack of hardware capacity, running out of disk space, software patches that  
27  
28

1 impacted the stability of the environment, poor system monitoring and an unskilled  
2 support team.”

3  
4 54. SPE has also failed to vigilantly employ intrusion prevention and  
5 detection protocols that would have prevented and immediately detected the breach in  
6 November 2014. Some experts who have analyzed the malicious software behind the  
7 Data Breach have suggested that the hackers may have been inside SPE’s network for  
8 some time, allowing them to become familiar with the network.  
9

10 55. Several security firms have noted that the data released by the hackers  
11 included a number of SPE’s private cryptographic keys. Kevin Bocek, vice president  
12 at Venafi, explained to Businessweek that losing control of these cryptographic “keys  
13 to the kingdom” is “a big deal.” A hacker who has access to the cryptographic keys  
14 can access encrypted servers without triggering intrusion detection systems because  
15 these systems assume the encrypted data is safe. Businessweek reported that an  
16 attack using cryptographic keys indicates that the hacker likely spent a significant  
17 amount of time within the company’s network. This is because companies are often  
18 slow to change their cryptographic keys, even when they are known to be vulnerable.  
19 Mr. Bocek noted that the 2011 PSN breach also compromised cryptographic keys,  
20 raising the question of why the Sony companies hadn’t established greater protection  
21 for them by 2014.  
22

23 56. Anyone with access to the cryptographic keys could access SPE’s  
24 network until the company changed them—a process made more difficult by the fact  
25  
26  
27  
28

1 that Sony apparently did not appropriately track the ways that cryptographic keys are  
2 used. For example, Kaspersky Lab pointed out that a sample of the malware that  
3 hackers installed on the SPE network during the Data Breach showed traces of being  
4 signed by a valid digital certificate from SPE. According to the cybersecurity firm:

6       The stolen Sony certificates (which were also leaked by the attackers)  
7       can be used to sign other malicious samples. In turn, these can be  
8       further used in other attacks. Because the Sony digital certificates are  
9       trusted by security solutions, this makes attacks more effective. We've  
10       seen attackers leverage trusted certificates in the past, as a means of  
11       bypassing whitelisting software and default-deny policies.

11       57. SPE's ability to prevent further unauthorized access to its network has  
12       been severely compromised given the hacker's access to and ability to release the  
13       cryptographic keys. In addition, ARS Technica reported that the hackers were able to  
14       collect significant intelligence on the network from SPE's own information  
15       technology department, including lists of all computers on SPE's internal networks.  
16       Among the files publicly disclosed the second week of December 2014 was a  
17       corporate certificate authority that was intended to be used in creating server  
18       certificates for SPE's Information Systems Service (ISS) infrastructure. This  
19       corporate certificate authority may have been used to create the server certificate that  
20       was used to sign a later version of the malware that took SPE's network offline as  
21       part of the Data Breach.  
22       part of the Data Breach.

26       58. Leaked emails from SPE's general counsel and chief compliance officer,  
27       Leah Weil, provided additional insight into SPE's deficient security practices.  
28       Among other topics, the emails voiced concerns about the volume of data available



1 on emails and SPE’s email retention policies. For example, one of Ms. Weil’s emails  
2 reportedly stated, “[w]hile undoubtedly there will be emails that need to be retained  
3 or stored electronically in a system other than email, many can be deleted, and I am  
4 informed by our IT colleagues that our current use of the email system for virtually  
5 everything is not the best way to do this.”  
6

7  
8 59. SPE has claimed that the Data Breach was “unprecedented in nature”  
9 and “undetectable by industry standard antivirus software.” The actual details tell a  
10 very different story. As Adam Caudill, an independent security researcher, suggests,  
11 “[t]o protect their image, [SPE] need[s] this to be an unpreventable, incredibly  
12 sophisticated attack.” But the hackers’ ongoing conduct should not have remained  
13 undetected, he explains: “Even if they couldn’t detect the malware, they should have  
14 detected the unusual activity. You don’t steal such a large amount of data without  
15 raising some red flags—the question is, was anyone watching?”  
16  
17

18  
19 60. Mike Gillepsie of Computer Weekly noted that “[t]his was a sustained  
20 attack of various visits and Sony was not aware until it was pointed out, and that is  
21 worth discussing.” He added, “[o]nce the attackers had found their way in, they took  
22 time to build a picture of the network architecture and then returned at a future point  
23 to attack specific servers—stealing information and then deleting the original files  
24 with sophisticated malware.” Mr. Gillepsie pointed out that a major security issue the  
25 Data Breach exposed was the lack of “effective segregation of data,” a problem that  
26  
27  
28 “seems to be across the corporation as the hackers were able to easily move between

1 areas, taking whatever they picked. ... The lack of segregation of data is a very poor  
2 security hygiene and given the details released by the hackers of usernames and  
3 passwords, this was not the only neglected area of security hygiene at Sony.” It is not  
4 yet known how the hackers actually breached the network, “but once inside, Sony  
5 certainly made it easy for them to move around and take what they wanted with  
6 impunity.” Philip Lieberman, the president of security management firm Lieberman  
7 Software, said: “It’s obvious from the scope of what’s been done that the intruders  
8 owned the entire environment . . . . Sony lost control of their environment.”

9  
10  
11  
12 **D. Current and Former SPE Employees Are Victims of the Breach**

13 61. In addition to implementing a sophisticated public relations campaign to  
14 portray the breach as beyond its control, SPE focused its early remediation efforts,  
15 *not* on protecting its employees and their families affected by the Data Breach, but  
16 rather on controlling the damage associated with unflattering comments in emails  
17 about movie stars and politicians and removing pirated films from the internet. SPE  
18 used hacking methods of its own to combat illegal downloads of its movies that the  
19 hackers publicly released.  
20  
21

22 62. Meanwhile, SPE failed to provide its current and former employees with  
23 concrete information about the breach, what data was exposed, and how SPE will  
24 protect their information going forward. Employees who called and emailed SPE  
25 were routinely ignored or given rote and unhelpful responses. One employee said,  
26  
27  
28

1 “We got more information from blogs and websites than we did from Michael  
2 [Lynton, CEO of SPE] and Amy [Pascal, co-chair of SPE].”  
3

4 63. It was not until the evening of December 2, 2014—more than a week  
5 after the breach was revealed—that SPE finally issued an official internal memo to  
6 6,500 employees confirming that the Data Breach was authentic, and “that a large  
7 amount of confidential Sony Pictures Entertainment data has been stolen by the cyber  
8 attackers, including personnel information and business documents.” SPE advised  
9 employees “to assume that information about you in the possession of the company  
10 might be in [the hackers’] possession.”  
11

12  
13 64. SPE sent a second company-wide memo to employees on December 8,  
14 assuring them that SPE was doing everything it could to protect them, stating that the  
15 FBI has “dedicated their senior staff to this global investigation” and that “recognized  
16 experts are working on this matter and looking out for our security.”  
17

18  
19 65. In another memo to employees about the Data Breach dated December  
20 8, 2014, SPE advised that it “believes that the following types of personally  
21 identifiable information that you provided to SPE may have been obtained by  
22 unauthorized individuals: (i) name, (ii) address, (iii) Social Security number, driver’s  
23 license number, passport number, and/or other government identifier, (iv) bank  
24 account information, (v) credit card information for corporate travel and expense, (vi)  
25 username and passwords, (vii) compensation and (viii) other employment related  
26 information. In addition, unauthorized individuals may have obtained (ix) HIPAA  
27  
28

1 protected health information, such as name, Social Security number, claims appeals  
2 information you submitted to SPE (including diagnosis and disability code), date of  
3 birth, home address, and member ID number to the extent that you and/or your  
4 dependents participated in SPE health plans, and (x) health/medical information that  
5 you provided to us outside of SPE health plans.” SPE warned its employees “to be  
6 especially aware of email, telephone, and postal mail scams that ask for personal or  
7 sensitive information” and “to remain vigilant, review your account statements,  
8 monitor your credit reports and change your passwords” to “protect against possible  
9 identity theft or other financial loss.”

10  
11  
12  
13 66. SPE has yet to notify all of its former employees about the breach and  
14 the extent of their data that was exposed. While several former SPE employees  
15 reported seeing their personal data in leaked documents by December 8, 2014, one  
16 former high-ranking employee who left the company earlier in the year told CNET  
17 that “[t]he studio’s done absolutely nothing to reach out to us.”  
18  
19

20 67. SPE posted a “message” for current and former employees on its website  
21 on December 15, 2014 advising that “the security of certain personally identifiable  
22 information about its current and former employees, and their dependents that  
23 participated in SPE health plans and other benefits, may have been compromised.”  
24 SPE said that it “has continued to engage in an effort to reach out to potentially  
25 impacted individuals with notification about this situation.” SPE later sent this  
26 message to some, but not all, former employees.  
27  
28

1           68. As a result of SPE's negligent security practices and slow response to  
2 the breach, SPE's current and former employees and their family members are  
3  
4 subject to an increased and concrete risk of identity theft due to the exposure of their  
5 financial, medical and other personal information and they have spent and will have  
6 to continue to spend substantial time and money securing their personal information  
7  
8 and accounts and protecting their identities.

9           69. An identity thief uses another's personal and financial information, such  
10 as the person's name, address, and other information, without permission, to commit  
11 fraud or other crimes. Identity thieves may commit various types of crimes, from  
12 immigration fraud, obtaining a driver's license or identification card in the victim's  
13 name, using the victim's information to obtain government benefits, to filing a  
14 fraudulent tax return using the victim's information to obtain a refund. Identity  
15 thieves may also obtain medical services using stolen medical data or commit any  
16 number of other frauds, such as obtaining a job, procuring housing or even giving  
17 false information to police during an arrest. They can also use victims' personal  
18 information to open new financial accounts and incur charges in another person's  
19 name, take out loans in another person's name, and incur charges on existing  
20 accounts.  
21  
22  
23  
24

25           70. There is a strong likelihood that current and former SPE employees, as  
26 well as their family members, are already or will become victims of identity fraud  
27 given the breadth of information about them that is now publicly available. Javelin  
28

1 Strategy & Research reported in its 2014 Identity Fraud Study that “[d]ata breaches  
2 are the greatest risk factor for identity fraud.” In fact, “[i]n 2013, one in three  
3 consumers who received notification of a data breach became a victim of fraud.”  
4 Javelin also found increased instances of fraud other than credit card fraud, including  
5 “compromised lines of credit, internet accounts (e.g., eBay, Amazon) and email  
6 payment accounts such as PayPal.”  
7  
8

9         71. As SPE itself recommended, current and former SPE employees and  
10 their family members will have to monitor their accounts and credit, and will also  
11 have to pay for credit monitoring or credit reports to make sure their credit and  
12 identity is not harmed by thieves. Individuals whose bank information was  
13 compromised may have to pay fees to their banks for new debit and credit cards, or  
14 have to pay fees to have the cards shipped faster so that they do not have to wait  
15 weeks to make purchases on their accounts. These individuals may also lose access  
16 to their funds and time and money by spending hours on the phone or in person with  
17 banks and credit agencies trying to reverse unauthorized charges, clear up credit  
18 issues, and order new cards.  
19  
20  
21

22         72. The public exposure of the Social Security numbers of tens of thousands  
23 of SPE’s current and former employees creates serious problems. Neal O’Farrell, a  
24 security and identity theft expert for Credit Sesame calls a Social Security number  
25 “your secret sauce,” that is “as good as your DNA to hackers.” Current and former  
26 employees have spent time contacting law enforcement and various agencies, such as  
27  
28

1 the Internal Revenue Service and the Social Security Administration, about the theft  
2 of their Social Security numbers. They have already experienced identity theft,  
3 identity or medical fraud, and/or now face a real and immediate risk of identity theft  
4 and other problems associated with the disclosure of their Social Security numbers,  
5 and will need to monitor their credit and tax filings for an indefinite duration. Yet,  
6 they will have to wait until they become victims of Social Security number misuse  
7 before they can obtain a new one. Even then, the Social Security Administration  
8 warns “that a new number probably will not solve all [] problems . . . and will not  
9 guarantee [] a fresh start.” In fact, “[f]or some victims of identity theft, a new  
10 number actually creates new problems.” One of those new problems is that a new  
11 Social Security number will have a completely blank credit history, making it  
12 difficult to get credit for a few years unless it is linked to the old compromised  
13 number.  
14  
15  
16  
17

18 73. Current and former SPE employees and family members whose medical  
19 and insurance information has been leaked will need to spend time monitoring their  
20 financial statements, medical bills, insurance records, utility bills and credit reports  
21 for the rest of their lives. They may also be fraudulently charged for unauthorized  
22 medical services or equipment, which will require them to spend time and money  
23 resolving these problems. They will also have to deal with an increased risk of  
24 medical identity theft. Medical information is highly valuable and is reportedly  
25 “worth 10 times more than [a person’s] credit card number on the black market.” The  
26  
27  
28

1 Office of Inspector General of the U.S. Department of Health & Human Services  
2 cautions that “[m]edical identity theft can disrupt your life, damage your credit rating,  
3 and waste taxpayer dollars. The damage can be life-threatening to you if the wrong  
4 information ends up in your personal medical records.”  
5

6 74. SPE has offered current and former employees twelve months of credit  
7 monitoring and identity theft insurance with AllClear ID. But, neither the monitoring  
8 nor the insurance can prevent identity theft or fraud, even for the twelve month  
9 period. Credit monitoring only informs a consumer of instances of fraudulent  
10 opening of new accounts. Identity theft insurance only reimburses losses after they  
11 have occurred. Neither of those services prevent identity theft or fraud by: (i)  
12 detecting sales of PII on underground black market websites before the PII is used to  
13 commit identity theft or identity fraud; (ii) monitoring public records, loan data, or  
14 criminal records; (iii) flagging existing accounts for fraud in order to thwart identity  
15 thieves’ use of compromised PII before an unauthorized transaction can be  
16 completed; or (iv) freezing credit, which prevents identity thieves’ ability to open  
17 new accounts with compromised PII.  
18  
19  
20  
21

22 75. Sites ranking companies that provide identity protection services have  
23 noted that while many of these companies do offer services to prevent identity theft  
24 and fraud, AllClear ID’s services only assist people that are *already* victims of  
25 identity thieves. In fact, these ranking sites regularly give seven or more other  
26  
27  
28



1 identity services companies a better overall ranking for identity services than  
2 AllClear ID.  
3

4 76. United States government and privacy experts acknowledge that it may  
5 take years for identity theft to come to light and be detected. As Identity Finder LLC  
6 CEO Todd Feinman told Law360, the real victims are SPE's current and former  
7 employees: "They're now at risk for identity theft for the rest of their lives."  
8

9 **VI. PLAINTIFFS' MOST SENSITIVE INFORMATION IS BREACHED,**  
10 **CAUSING LIFELONG DATA INSECURITY**

11 **A. Michael Corona**

12 77. Plaintiff Michael Corona is a former employee of SPE, which employed  
13 Plaintiff Corona from 2004 to 2007 in Culver City, California. He is currently a  
14 resident of the State of Virginia.  
15

16 78. In exchange for his employment services, SPE offered to compensate  
17 Plaintiff Corona and provide him with other employment benefits. To receive  
18 compensation and employment benefits, SPE required Plaintiff Corona to: (i) provide  
19 SPE with PII to fulfill SPE's legal responsibilities and operational requirements,  
20 including his full name, home address, Social Security Number, as well as PII of  
21 people designated as beneficiaries on his employment-related benefits through SPE;  
22 (ii) cooperate in providing medical information necessary to determine responsibility  
23 for health provider payments; and (iii) provide other confidential information  
24 including self-evaluations and, ultimately, his reason for resigning. Plaintiff Corona  
25 believes that this was a standard employment agreement that SPE had with its  
26  
27  
28

1 employees during his tenure at SPE. Plaintiff Corona accepted SPE's employment  
2 offer and provided the PII SPE required, expecting that SPE would exercise  
3 reasonable care to safeguard and maintain the confidentiality of his PII except to the  
4 extent necessary to provide the agreed compensation and other employment benefits.  
5 When he ended his employment with SPE, he expected that SPE would destroy or  
6 archive his information securely.  
7

9 79. Plaintiff Corona contacted SPE's human resources department on or  
10 about December 2, 2014 after hearing about the Data Breach seeking to learn whether  
11 his PII had been compromised. While SPE confirmed receipt of his inquiry, to date,  
12 SPE has not substantively responded to his inquiry.  
13

14 80. Due to SPE's silence, Plaintiff Corona spent 40-50 hours confirming for  
15 himself whether the Data Breach compromised his PII, and, on or about December 7,  
16 2014, Plaintiff Corona was able to confirm that his PII was compromised as a result  
17 of the Data Breach and that an unencrypted spreadsheet containing his PII had been  
18 publicly distributed on the internet, including, but not limited to, his full name, Social  
19 Security Number, birthdate, former home address, salary history, and reason for  
20 resigning. In addition, due to media reports of medical data and policy numbers  
21 being compromised in the Data Breach and his knowledge of SPE correspondence  
22 relating to health care provided to him while employed at SPE, Plaintiff Corona  
23 believes that his medical information was also compromised by the Data Breach.  
24  
25  
26  
27  
28

1           81. Upon confirming that his PII was compromised, Plaintiff Corona spent  
2 an additional 40-50 hours attempting to contain the impact of the Data Breach on his  
3 and his family's identity through the end of December 2014. On or about December  
4 7, 2014, Plaintiff Corona signed up with LifeLock identity protection, monitoring,  
5 and recovery services for himself and his family, causing him to incur annual out-of-  
6 pocket costs of approximately \$700 per year. He then subsequently continued to  
7 research ways to contain the impact of SPE's Data Breach on himself and his family  
8 members, including: (i) spending hours changing passwords and meticulously  
9 combing through emails to delete those containing PII beyond his name and email  
10 address; (ii) transferring financial, retirement, utility, and other accounts and/or  
11 obtaining new PINs for these accounts; (iii) placing a fraud alert with a credit agency;  
12 (iv) learning through his continued research on December 9, 2014 about an SPE  
13 email in which SPE former employees could be requested to be added to the AllClear  
14 ID program and requesting inclusion in the program; (v) receiving confirmation on  
15 December 10, 2014 that SPE had submitted his information to AllClear ID, but  
16 needing to contact AllClear ID directly to initiate services; (vi) subsequently  
17 contacting AllClear ID to initiate services; (vii) contacting law enforcement  
18 authorities pertaining to his compromised PII as a result of the Data Breach; and (viii)  
19 filing a complaint with the Federal Trade Commission pertaining to his compromised  
20 PII as a result of the Data Breach. If SPE had proactively notified him of the Data  
21 Breach and/or responded to his inquiry attempting to confirm that the Data Breach

1 compromised his PII, he would have attempted to further contain the impact of SPE's  
2 Data Breach on his PII by taking these steps sooner.

3  
4 82. Despite Plaintiff Corona's efforts to contain the impact of SPE's Data  
5 Breach on his PII, Plaintiff Corona received further confirmation that his PII had not  
6 only been compromised and publicized as a result of the Data Breach, but that an  
7 identity thief had used his compromised PII to attempt to open a new bank account.  
8 AllClear ID notified him on December 20, 2014 that because Plaintiff Corona had  
9 independently acted to place a 90-day fraud alert with a credit agency, the thief's  
10 attempt to open the account had been thwarted this time. Nevertheless, Plaintiff  
11 Corona understands that he will need to be diligent and renew this fraud alert with a  
12 credit agency every 90 days to retain this preventative protection. Going forward,  
13 Plaintiff Corona anticipates spending considerable time and money for the rest of his  
14 life in order to contain the impact of SPE's Data Breach on himself and his family  
15 members, and people designated as beneficiaries on his employment-related benefits  
16 through SPE.

17  
18  
19  
20  
21 **B. Christina Mathis**

22 83. Plaintiff Christina Mathis is a former employee of Sony Pictures  
23 Consumer Products, a subsidiary of SPE, which employed Plaintiff Mathis from  
24 approximately 2000 to 2002 in Culver City, California. She is currently a resident of  
25 the State of California. Plaintiff Mathis has not worked for Sony in over 12 years.  
26  
27  
28

1           84. In exchange for her employment services, SPE offered to compensate  
2 Plaintiff Mathis and provide her with other employment benefits. To receive  
3 compensation and employment benefits, SPE required Plaintiff Mathis to provide  
4 SPE with PII to fulfill SPE's legal responsibilities and operational requirements,  
5 including her full name, Social Security Number, home address, as well as PII of  
6 beneficiaries of her employment-related benefits through SPE. Plaintiff Mathis  
7 accepted SPE's employment offer and provided the PII SPE required, expecting that  
8 SPE would exercise reasonable care to safeguard and maintain the confidentiality of  
9 her PII except to the extent necessary to provide the agreed compensation and other  
10 employment benefits. When she ended her employment with SPE, she expected that  
11 SPE would destroy or archive her information securely.  
12

13  
14  
15  
16           85. Plaintiff Mathis learned about the Data Breach through the Huffington  
17 Post on or about December 1, 2014, but believed that the Data Breach compromised  
18 only the PII of current SPE employees. On or about December 11, 2014, her further  
19 investigation uncovered an email address for former employees that she used to  
20 contact SPE seeking to confirm whether her PII had been compromised and to  
21 request SPE assistance in containing compromised PII.  
22  
23

24           86. Despite the fact that she has not worked at SPE for 12 years, on or about  
25 December 11, 2014, Plaintiff Mathis was able to confirm through a non-SPE source  
26 that her PII was compromised as a result of the Data Breach and that her PII was  
27  
28

1 publicly available on the internet, including but not limited to her full name, Social  
2 Security Number and prior home address.

3  
4 87. Upon confirming that her PII had been compromised and published to  
5 the internet, Plaintiff Mathis spent time enrolling in LifeLock identity protection,  
6 monitoring, and recovery services for herself, causing her to incur annual out-of-  
7 pocket costs of approximately \$300. She subsequently spent many hours continuing  
8 to research ways to contain the impact of SPE's Data Breach on her PII, including: (i)  
9 contacting her bank to alert them to the compromise of her PII as a result of SPE's  
10 Data Breach; (ii) contacting a password protection entity and paying \$29.99 to  
11 change and manage all of her new passwords; (iii) increasing privacy screens on  
12 social media sites; and (iv) placing a 90-day credit fraud alert with a credit service  
13 entity. If SPE had proactively notified her of the Data Breach and/or substantively  
14 responded to her inquiry attempting to confirm that the Data Breach compromised her  
15 PII, she would have attempted to further contain the impact of SPE's Data Breach on  
16 her PII by taking these steps sooner.

17  
18  
19  
20  
21 88. On or about December 18, 2014, Plaintiff Mathis received an email from  
22 SPE stating that it was providing AllClear ID's Secure and PRO services for 12  
23 months from the date of the email, which would automatically provide an identity  
24 theft investigator if a problem arose, and that she could use a redemption code to sign  
25 up for AllClear ID. The email also recommended that Plaintiff Mathis regularly  
26 review statements from her accounts and periodically obtain her credit report for  
27  
28

1 accounts and creditor inquiries that she did not recognize, as well as home addresses  
2 and Social Security numbers that were not accurate. It further recommended that she  
3 remain vigilant with respect to reviewing her account statements and credit reports  
4 and report suspected identity theft to proper law enforcement authorities, including  
5 local law enforcement, the state attorney general and/or the Federal Trade  
6 Commission. SPE also recommended that she regularly review her explanation of  
7 benefits statements from her insurer for unrecognized medical bills. Accordingly,  
8 going forward, Plaintiff Mathis anticipates spending considerable time and money for  
9 the rest of her life in an effort to contain the impact of SPE's Data Breach on herself  
10 and people designated as beneficiaries on her employment-related benefits through  
11 SPE.  
12  
13  
14  
15

16 **C. Joshua Forster**

17 89. Plaintiff Joshua Forster is a former employee of Sony Pictures  
18 Imageworks, a division of SPE, which employed Plaintiff Forster from approximately  
19 January 2013 to April 2013 in California. In addition, Plaintiff Forster worked for  
20 SPE as a contractor from approximately April 2013 until February 2014, and worked  
21 on and off for various SPE subsidiaries and affiliates from approximately June 2004  
22 to August 2010. He is currently a resident of the State of Colorado.  
23  
24

25 90. In exchange for his employment services, SPE offered to compensate  
26 Plaintiff Forster and provide him with other employment benefits. To receive  
27 compensation and employment benefits, SPE required Plaintiff Forster to: (i) provide  
28

1 SPE with PII to fulfill SPE's legal responsibilities and operational requirements,  
2 including his: full name, home address, telephone number, date of birth, Social  
3 Security Number, direct deposit routing instructions, copies of his driver's license,  
4 Social Security card, and resident alien card, as well as PII of beneficiaries of his  
5 employment-related benefits through SPE; (ii) cooperate in providing information  
6 about his health condition to receive medical care from SPE's on-site medical  
7 facility; and (iii) provide other confidential information including his credit card  
8 information in order to make purchases from SPE's on-site store and information  
9 necessary for SPE to run a background check. Plaintiff Forster accepted SPE's  
10 employment offer and provided the PII SPE required, expecting that SPE would  
11 exercise reasonable care to safeguard and maintain the confidentiality of his PII  
12 except to the extent necessary to provide the agreed compensation and other  
13 employment benefits. When he ended his employment with SPE, he expected that  
14 SPE would destroy or archive his information securely.

15  
16  
17  
18  
19  
20 91. Plaintiff Forster learned of SPE's Data Breach from speaking with  
21 relatives who were employed by SPE at the time of the Data Breach on or about  
22 November 24, 2014, and later watching the news on television that reported on the  
23 Data Breach. Plaintiff Forster subsequently spent approximately 15 hours further  
24 investigating the Data Breach and obtained SPE files that were publicly available on  
25 the internet, on or about December 6, 2014, from which he confirmed that the Data  
26 Breach had compromised his PII, including his name, home address, Social Security  
27  
28



1 Number, date of birth, telephone number, SPE title, salary, the management structure  
2 of his SPE group, and information regarding the insurance carrier, plan, and  
3 premiums paid for his medical insurance coverage provided through SPE as a  
4 dependent of another SPE employee.  
5

6 92. Plaintiff Forster's further investigation uncovered information, on or  
7 about December 8, 2014, of an email address that he used to contact SPE seeking  
8 SPE's assistance in containing compromised PII. SPE informed Plaintiff Forster, on  
9 or about December 9, 2014, that AllClear ID would contact him with further  
10 information, which was ultimately provided by email on December 12, 2014 along  
11 with a redemption code for 12 months of AllClear ID credit monitoring at SPE's  
12 expense. Plaintiff Forster also spent time cancelling credit cards, obtaining new  
13 credit cards and resetting automatic billing instructions, as well as contacting a credit  
14 bureau to set up fraud alerts during this timeframe. If SPE had notified him earlier  
15 about the Data Breach and provided him information on how to contain the potential  
16 compromise of his PII, Plaintiff Forster would have been able to take these steps to  
17 contain the compromise of his PII more quickly.  
18  
19  
20  
21

22 93. Despite Plaintiff Forster's efforts to contain the compromise of his PII,  
23 he learned in or about January 2015 that someone was using his PII to attempt to  
24 open a PayPal credit card under his name. While Plaintiff Forster had previously  
25 used the AllClear ID redemption code to obtain credit monitoring, he did not learn of  
26 the unauthorized use of his PII from AllClear ID, but from PayPal. Plaintiff Forster  
27  
28

1 then contacted AllClear ID to let it know of this unauthorized use of his PII, which  
2 informed him that because one of the credit bureau agencies did not have his date of  
3 birth on file, AllClear ID could not confirm his identity and therefore had not initiated  
4 his subscription. Prior to Plaintiff Forster contacting AllClear ID, AllClear ID had  
5 not attempted to contact him about his registration issues. Plaintiff Forster ultimately  
6 received confirmation of his registration for AllClear ID credit monitoring on or  
7 about January 20, 2015, about a month after he had used his redemption code to sign  
8 up for AllClear ID credit monitoring.  
9

10  
11  
12 94. Plaintiff Forster continued his efforts to contain the compromise of his  
13 PII in late January 2015 by changing his bank account information, which required  
14 multiple personal visits to his bank because his account was linked to a relative's  
15 account who lives over a thousand miles away and both Plaintiff Forster and his  
16 relative needed to be personally present for the bank to change this information.  
17  
18 Going forward, Plaintiff Forster anticipates spending considerable time and money  
19 for the rest of his life in order to contain the impact of SPE's Data Breach on himself,  
20 his relative that was linked to his bank account, and people designated as  
21 beneficiaries on his employment-related benefits through SPE.  
22  
23

24 **D. Ella Carline Archibeque**

25 95. Plaintiff Ella Carline Archibeque is a former employee of Sony Pictures  
26 Imageworks, a division of SPE, which employed Plaintiff Archibeque at various  
27  
28

1 times from approximately April 2002 through May 2009 in Culver City, California.

2 She is currently a resident of the State of California.

3  
4 96. In exchange for her employment services, SPE offered to compensate  
5 Plaintiff Archibeque and provide her with other employment benefits. To receive  
6 compensation and employment benefits, SPE required Plaintiff Archibeque to  
7 provide SPE with PII to: (i) fulfill SPE's legal responsibilities and operational  
8 requirements, including her name, home address, email address, Social Security  
9 Number, date of birth, copy of her passport and driver's license, IRS W-4 Employee  
10 Withholding Allowance Certification information (including marital status), and bank  
11 routing information, as well as PII of designated beneficiaries on her employment-  
12 related benefits plans offered through SPE, (ii) obtain medical insurance offered by  
13 SPE as an employment benefit; and (iii) other confidential information including  
14 information needed for SPE to obtain a background check. Plaintiff Archibeque  
15 accepted SPE's employment offer and provided the PII SPE required, expecting that  
16 SPE would exercise reasonable care to safeguard and maintain the confidentiality of  
17 her PII except to the extent necessary to provide the agreed compensation and other  
18 employment benefits. When she ended her employment with SPE, she expected that  
19 SPE would destroy or archive her information securely.

20  
21 97. Plaintiff Archibeque first heard about the Data Breach in late November  
22 2014. As the media continued to report on the increasing scope of the Data Breach in  
23 early December, SPE remained silent about its extent. Plaintiff Archibeque acted to  
24

1 contain the potential impact of the Data Breach on her PII. For example, she enrolled  
2 in LifeLock identity protection, monitoring, and recovery services for herself, in or  
3 about early December, causing her to incur annual out-of-pocket costs of  
4 approximately \$240 per year. As she continued to investigate published information  
5 about the Data Breach, she obtained an email address designated for former  
6 employees to contact SPE about the Data Breach. She then contacted SPE by email,  
7 on or about December 9, 2014, at this address, seeking to confirm whether the Data  
8 Breach had compromised her PII. SPE responded to her email, on or about  
9 December 10, 2014, with an AllClear ID offer.

13 98. Despite Plaintiff Archibeque's efforts to contain the impact of SPE's  
14 Data Breach on her PII, Plaintiff Archibeque received confirmation that her PII had  
15 not only been compromised and publicized as a result of the Data Breach, but that her  
16 PII was being sold on the black market. On December 10, 2014, LifeLock provided  
17 Plaintiff Archibeque with a Black Market Website Notification which stated that  
18 LifeLock had detected that her email address and password was being sold on a black  
19 market website. In response to this notification, she has frozen her credit, and placed  
20 a fraud alert with the Internal Revenue Service and a credit agency. If SPE had  
21 proactively notified Plaintiff Archibeque about the Data Breach, she would have  
22 attempted to further contain the impact of SPE's Data Breach on her PII by taking  
23 these steps sooner. Going forward, Plaintiff Archibeque anticipates spending  
24 considerable time and money for the rest of her life in an effort to contain the impact

1 of SPE's Data Breach on herself and people designated as beneficiaries on her  
2 employment-related benefits through SPE.  
3

4 **E. Michael Levine**

5 99. Plaintiff Michael Levine is a former employee of Sony Pictures  
6 Imageworks, a division of SPE, which employed Plaintiff Levine from approximately  
7 2003 to 2012 in California. He is currently a resident of California.  
8

9 100. In exchange for his employment services and consent to use his image  
10 for promotional purposes, SPE offered to compensate Plaintiff Levine and provide  
11 him with other employment benefits. To receive compensation and employment  
12 benefits, SPE required Plaintiff Levine to: (i) provide SPE with PII to fulfill SPE's  
13 legal responsibilities and operational requirements, including his: full name, home  
14 address, date of birth, Social Security Number, and direct deposit routing instructions,  
15 as well as PII of people designated as beneficiaries on his employment-related  
16 benefits through SPE; (ii) cooperate in providing medical information relevant to  
17 health insurance coverage; and (iii) provide other confidential information including  
18 his employment and educational history. Plaintiff Levine accepted SPE's  
19 employment offer and provided the PII SPE required, expecting that SPE would  
20 exercise reasonable care to safeguard and maintain the confidentiality of his PII  
21 except to the extent necessary to provide the agreed compensation and other  
22 employment benefits. When he ended his employment with SPE, he expected that  
23 SPE would destroy or archive his information securely.  
24  
25  
26  
27  
28

1           101. Plaintiff Levine learned of SPE's Data Breach, on or about the end of  
2 November 2014, through an article written in *Variety*. Plaintiff Levine subsequently  
3 spent approximately 40 hours further investigating the Data Breach during the next  
4 approximately two weeks and ultimately obtained the SPE master index file that was  
5 publicly available on the internet, from which he confirmed that the Data Breach had  
6 compromised his PII, including his name, employment offer letters, and payroll  
7 information, including his Social Security Number.  
8

9  
10           102. Within approximately a week of confirming that his PII had been  
11 compromised in the Data Breach, Plaintiff Levine continued investigating ways to  
12 contain the impact of the Data Breach on himself and family. He contacted SPE by  
13 sending three separate emails seeking guidance in relation to this issue, but received  
14 only a single generic response from SPE several weeks later offering 12 months of  
15 AllClear ID identity theft investigation and credit monitoring services at its expense  
16 to current and former employees with potentially compromised PII as a result of the  
17 Data Breach.  
18  
19  
20

21           103. While he was awaiting a response from SPE to his inquiries, Plaintiff  
22 Levine spent 30 to 40 hours continuing to investigate how to contain the impact of  
23 the SPE Data Breach on himself and his family, and acted to contain this impact by:  
24 (i) freezing his credit so that new credit card accounts could not be opened and new  
25 bank loans could not be obtained with his compromised PII, resulting in \$50 in out-  
26 of-pocket costs to date; (ii) upgrading his family's AAA membership to AAA Plus in  
27  
28

1 order to obtain monthly credit monitoring and credit fraud notification services, at an  
2 added annual expense of \$50; (iii) notifying the Internal Revenue Service that his  
3 Social Security Number had been compromised as a result of the Data Breach; and  
4 (iv) placing fraud alerts with Experian, Equifax, TransUnion, and his other financial  
5 accounts.  
6

7  
8 104. If SPE had proactively notified him of the Data Breach and promptly  
9 responded to his inquiries for more information, Plaintiff Levine would have been  
10 able to take these steps more quickly because he would not have had to spend so  
11 much time researching how to contain the impact of the Data Breach on himself and  
12 his family. Going forward, Plaintiff Levine anticipates spending considerable time  
13 and money for the rest of his life in an effort to contain the impact of SPE's Data  
14 Breach on himself, his family, and people designated as beneficiaries on his  
15 employment-related benefits through SPE.  
16  
17

18 **F. Geoffrey Springer**

19  
20 105. Plaintiff Geoffrey Springer is a former employee of SPE, which  
21 employed Springer from approximately October 1995 to August 1997 and again from  
22 approximately April 2000 through December 2004 in California. He is currently a  
23 resident of the State of Virginia.  
24

25 106. In exchange for his employment services and his agreement not to  
26 compete with SPE for a certain time period after leaving employment with SPE, SPE  
27 offered to compensate Plaintiff Springer and provide him with other employment  
28

1 benefits. To receive compensation and employment benefits, SPE required Plaintiff  
2 Springer to: (i) provide SPE with PII to fulfill SPE's legal responsibilities and  
3 operational requirements, including his full name, home address, Social Security  
4 Number, date of birth, bank account electronic deposit information, as well as PII of  
5 people designated as beneficiaries on his employment-related benefits through SPE;  
6 (ii) cooperate in providing medical information necessary to treat him in the event of  
7 a workplace medical emergency, including his health care providers and preferred  
8 hospital; and (iii) provide other confidential information including employment and  
9 education history. Plaintiff Springer accepted SPE's employment offer and provided  
10 the PII SPE required, expecting that SPE would exercise reasonable care to safeguard  
11 and maintain the confidentiality of his PII except to the extent necessary to provide  
12 the agreed compensation and other employment benefits. When he ended his  
13 employment with SPE, he expected that SPE would destroy or archive his  
14 information securely.

15  
16  
17  
18  
19  
20 107. Plaintiff Springer initially heard of SPE's Data Breach around  
21 Thanksgiving 2014, when he was watching news that included a report on the Data  
22 Breach. On or about the first week of December 2014, Plaintiff Springer obtained an  
23 unencrypted publicly available SPE file from the internet and confirmed that this file  
24 contained his PII, including his name, Social Security Number, home address during  
25 his employment at SPE, job title and date of separation from SPE.  
26  
27  
28



1           108. After Plaintiff Springer confirmed that the Data Breach had  
2 compromised his PII, he reached out to SPE's human resources department and  
3  
4 learned that SPE had created an email address box for former employees to contact in  
5 order to obtain one year of credit monitoring through AllClear ID at SPE's expense.

6           109. Plaintiff Springer then spent approximately 15 hours evaluating AllClear  
7 ID and other competing identity protection services, and concluded that paying to  
8 protect his PII through LifeLock would minimize his losses if his PII was to be used  
9 by an identity thief because it not only monitored credit reporting agencies, but also  
10 credit card purchasing information, bank account transactions, and scanned the dark  
11 web. On or about mid-December, Plaintiff Springer paid to obtain these services  
12 from LifeLock for himself, causing him to incur annual out-of-pocket costs of more  
13 than \$350 per year.  
14  
15

16           110. Plaintiff Springer subsequently spent approximately 40 hours continuing  
17 to research ways to contain the impact of SPE's Data Breach, including: placing a  
18 security freeze on his credit, making advance arrangements for a timeframe to unlock  
19 and re-freeze his credit so that he could purchase a vehicle, and paying \$30, so far, to  
20 freeze, unfreeze, and re-freeze his credit, placing fraud alerts with credit reporting  
21 agencies Experian, Equifax, and TransUnion, contacting the Internal Revenue Service  
22 and informing them that his Social Security Number had been compromised in the  
23 Data Breach, and resetting his car and mortgage automatic payment instructions. If  
24 SPE had notified him earlier about the Data Breach and provided him information on  
25  
26  
27  
28

1 how to contain the potential compromise of his PII, Plaintiff Springer would have  
2 been able to take these steps to contain the compromise of his PII more quickly.  
3

4 Going forward, Plaintiff Springer anticipates spending considerable time and money  
5 for the rest of his life in order to contain the impact of SPE's Data Breach on himself  
6 and people designated as beneficiaries on his employment-related benefits through  
7  
8 SPE.

9 **G. Marcela Bailey**

10 111. Plaintiff Marcela Bailey is a former employee of SPE, which employed  
11 Plaintiff Bailey from approximately January 1991 to February 2013. She is currently  
12 a resident of California.  
13

14 112. In exchange for her employment services, SPE offered to compensate  
15 Plaintiff Bailey and provide her with other employment benefits. To receive  
16 compensation and employment benefits, SPE required Plaintiff Bailey to provide SPE  
17 with PII to fulfill SPE's legal responsibilities and operational requirements, including  
18 (i): her name, home address, telephone number, Social Security Number, date of  
19 birth, marital status, signature, physical characteristics description, passport number,  
20 copy of her Visa, driver's license number, direct deposit routing instructions, as well  
21 as PII of her dependents and people designated as beneficiaries on her employment-  
22 related benefits through SPE; (ii) medical and health insurance information; and (iii)  
23 other confidential information including education and employment history, financial  
24 information including credit card numbers and investment information, personnel file  
25  
26  
27  
28

1 information, passwords, and educational information for tuition reimbursement.

2 Plaintiff Bailey accepted SPE's employment offer and provided the PII SPE required,  
3  
4 expecting that SPE would exercise reasonable care to safeguard and maintain the  
5 confidentiality of her PII and other confidential information except to the extent  
6 necessary to provide the agreed compensation and other employment benefits. When  
7 she ended her employment with SPE, she expected that SPE would destroy or archive  
8 her information securely.  
9

10 113. On or about November 24, 2014, Plaintiff Bailey received three  
11 automated pre-recorded calls from SPE's emergency notification line throughout the  
12 day. Although Plaintiff Bailey is a former employee, she nevertheless received these  
13 calls because SPE had not removed Plaintiff Bailey from its employee emergency  
14 notification list. The recordings, which were presumably made to all current SPE  
15 employees, only instructed SPE employees to shut down their computers and log off  
16 until further notice. Upon hearing the recording, Plaintiff Bailey emailed SPE  
17 requesting that she be removed from SPE's emergency employee notification list as  
18 she was no longer an employee. After Plaintiff Bailey's email bounced back as  
19 undeliverable, Plaintiff Bailey contacted a member of SPE responsible for overseeing  
20 the emergency phone system asking to be removed from the call list. Plaintiff Bailey  
21 received a response that evening stating that she would be removed and stating that  
22 there was a major hack, but no mention was made that her PII had been or was in  
23  
24  
25  
26  
27  
28

1 danger of being disclosed. Throughout the evening, Plaintiff Bailey also had heard  
2 various breaking news reports regarding the security breach at SPE.  
3

4 114. Due to SPE's failure to substantively respond to her inquiries and update  
5 her with information, Plaintiff Bailey expended 30 to 40 hours and incurred expenses  
6 attempting to protect her and her family's PII from unauthorized use, including:  
7 purchasing LifeLock's identity theft protection services for her family on or about  
8 December 15, 2014, for which she has incurred out-of-pocket expenses of over \$1000  
9 and will incur out-of-pocket expenses of more than \$1000 annually, monitoring and  
10 changing bank and credit accounts, placing credit freezes, and closely monitoring  
11 news coverage and reports pertaining to the breach.  
12  
13

14 115. Despite her efforts to contain the impact of the Data Breach on the PII of  
15 her family and herself, Plaintiff Bailey received confirmation that her PII was being  
16 sold on the black market. On or about December 17, 2014, Plaintiff Bailey received a  
17 black market alert from LifeLock that notified her that her name and Social Security  
18 Number were being sold on an illegal black market website.  
19  
20

21 116. Plaintiff Bailey received further confirmation that her family's PII had  
22 not only been compromised in the Data Breach, but was also being used by an  
23 identity thief. Specifically, an identity thief appears to have succeeded in making  
24 unauthorized cash withdrawals on her husband's bank account, causing her family to  
25 incur overdraft charges and spending 10 hours making a claim and replacing the  
26 affected debit card.  
27  
28

1           117. Going forward, Plaintiff Bailey anticipates spending considerable time  
2 and money for the rest of her life in an effort to contain the impact of SPE's Data  
3 Breach on herself, her family, and people designated as beneficiaries on her  
4 employment-related benefits through SPE.  
5

6           **H. Steven Shapiro**  
7

8           118. Plaintiff Steven Shapiro is a former employee of Sony Pictures  
9 Imageworks, a division of SPE, which employed Plaintiff Shapiro from  
10 approximately October 2003 through January 2010 in California. He is currently a  
11 resident of California.  
12

13           119. In exchange for his employment services, SPE offered to compensate  
14 Plaintiff Shapiro and provide him with other employment benefits. To receive  
15 compensation and employment benefits, SPE required Plaintiff Shapiro to provide  
16 SPE with PII to fulfill SPE's legal responsibilities and operational requirements,  
17 including: (i) his full name, home address, Social Security Number, copy of his  
18 driver's license and passport, bank wiring instructions for direct deposits, as well as  
19 PII of people designated as beneficiaries on his employment-related benefits through  
20 SPE; and (ii) medical information about major procedures and medical insurance  
21 claims. Plaintiff Shapiro accepted SPE's employment offer and provided the PII SPE  
22 required, expecting that SPE would exercise reasonable care to safeguard and  
23 maintain the confidentiality of his PII except to the extent necessary to provide the  
24 agreed compensation and other employment benefits. When he ended his  
25  
26  
27  
28

1 employment with SPE, he expected that SPE would destroy or archive his  
2 information securely.  
3

4 120. Plaintiff Shapiro first learned of the Data Breach from an online media  
5 site that SPE employee data was compromised by the Data Breach on or about  
6 November 27, 2014.  
7

8 121. Plaintiff Shapiro thus contacted SPE on or about December 5, 2014  
9 seeking to confirm whether his PII had been compromised as a result of the Data  
10 Breach and sought to learn how to contain the potential damage to his identity. SPE  
11 acknowledged Plaintiff Shapiro's inquiry on December 8, 2014, and told him that it  
12 may take several days for SPE to substantively respond. On December 11, 2014,  
13 SPE informed him that it was working to provide 12 months of AllClear ID credit  
14 monitoring services, at SPE's expense, to potentially impacted employees and former  
15 employees (and their dependents), but, would not be offering these services to named  
16 beneficiaries who are not dependents of employees or former employees. To date,  
17 SPE has not confirmed whether or not Plaintiff Shapiro's PII was in fact  
18 compromised through the Data Breach.  
19  
20  
21  
22

23 122. Due to SPE's delay and failure to date to substantively respond to his  
24 inquiry, Plaintiff Shapiro has spent between 100 and 150 hours confirming whether  
25 the Data Breach compromised his PII over several weeks. He ultimately obtained  
26 SPE files that were publicly available on the internet that confirmed that his PII,  
27 including his name, address, Social Security Number, salary, reason for leaving SPE,  
28

1 position, and checking account information, was compromised and released as a  
2 result of the Data Breach in or about mid-December 2014. Plaintiff Shapiro also  
3 confirmed that this information was available for anyone to download, including  
4 anyone who would want to sell it on the black market. Plaintiff Shapiro also believes  
5 that his medical information may have been compromised because he heard that  
6 medical information regarding major medical procedures performed on SPE  
7 employees was also compromised in the Data Breach.  
8

9  
10 123. Plaintiff Shapiro subsequently spent significant time attempting to  
11 contain the impact of the compromised PII on his identity by: (i) spending  
12 approximately four hours placing a credit freeze with four credit bureaus, requiring  
13 him to pay \$40; (ii) spending approximately 30 hours managing the aftermath of his  
14 credit being frozen, including difficulty setting up new utilities after moving and  
15 problems obtaining a lease for a new home, which has required him to pay \$30 to  
16 unfreeze his credit; (iii) paying \$50 to obtain all of his credit reports and credit scores  
17 which were required by his new landlord because of difficulties that his landlord had  
18 in reviewing his credit; and (iv) changing his bank account, which required spending  
19 time tracking outstanding checks from his old accounts that needed to be cashed  
20 before he could close it, as well as depositing a minimum deposit in his new account  
21 to avoid re-issued checking fees and updating all of his utilities and other vendors that  
22 were automatically billed and being paid from his prior bank account.  
23  
24  
25  
26  
27  
28

1           124. Going forward, Plaintiff Shapiro anticipates spending considerable time  
2 and money for the rest of his life in an effort to contain the impact of SPE's Data  
3 Breach on himself and people designated as beneficiaries on his employment-related  
4 benefits through SPE.  
5

6           **I. Lawon Exum**  
7

8           125. Plaintiff Lawon Exum is a former employee of SPE, which employed  
9 Plaintiff Exum from approximately 2005 to 2014 in Culver City, California. He is  
10 currently a resident of the State of California.  
11

12           126. In exchange for his employment services, SPE offered to compensate  
13 Plaintiff Exum and provide him with other employment benefits. To receive  
14 compensation and employment benefits, SPE required Plaintiff Exum to provide SPE  
15 with PII to fulfill SPE's legal responsibilities and operational requirements, including  
16 his full name, Social Security Number and home address, as well as PII of people  
17 designated as beneficiaries on his employment-related benefits through SPE.  
18 Plaintiff Exum accepted SPE's employment offer and provided the PII SPE required,  
19 expecting that SPE would exercise reasonable care to safeguard and maintain the  
20 confidentiality of his PII except to the extent necessary to provide the agreed-upon  
21 compensation and other employment benefits. When he ended his employment with  
22 SPE, he expected that SPE would destroy or archive his information securely.  
23  
24  
25  
26  
27  
28



1           127. Plaintiff Exum learned about the Data Breach on or about November 24,  
2 2014, and immediately sent an email to SPE to confirm whether his PII had been  
3 compromised and to request SPE's assistance in containing his compromised PII.  
4

5           128. Plaintiff Exum was able to confirm on or about December 12, 2014  
6 through investigation and filing his yearly income tax return, that his PII was  
7 compromised in the Data Breach and that the hackers publicly distributed his PII on  
8 the internet, including but not limited to his full name, Social Security number and  
9 home address.  
10

11           129. Upon confirming that his PII had been compromised, Plaintiff Exum  
12 spent approximately 80 hours contacting his creditors, financial institutions, and the  
13 three credit bureaus. A block was placed on his credit reports which led to a denial of  
14 credit. He was unable to open a checking account or receive further credit from his  
15 credit union due to the blocks placed on his credit reports. He incurred late/declined  
16 payment fees as a result of failed automatic payments. Additionally, he contacted the  
17 Culver City Police Department and the Internal Revenue Service to make them aware  
18 of the situation and to inquire about his PII being compromised. Plaintiff Exum  
19 incurred out-of-pocket costs of approximately \$500 in these efforts. If SPE had  
20 proactively notified him of the Data Breach or responded to his inquiry, he would  
21 have been able to take these steps sooner.  
22

23           130. On or about December 28, 2014, Plaintiff Exum received a letter from  
24 SPE written to provide employees information about the Data Breach. The letter was  
25  
26  
27  
28

1 dated December 17, 2014, but Plaintiff Exum did not receive it until December 28,  
2 2014. Going forward, Plaintiff Exum anticipates spending considerable time and  
3 money for the rest of his life in an effort to contain the impact of SPE's Data Breach  
4 on himself and people designated as beneficiaries on his employment-related benefits  
5 through SPE.  
6

## 7 **VII. CLASS ACTION ALLEGATIONS**

8  
9 131. Plaintiffs bring claims pursuant to Federal Rule of Civil Procedure 23 on  
10 behalf of classes of similarly situated persons, which they initially propose be defined  
11 as follows:  
12

### 13 **Nationwide Class**

14 All current and former SPE employees in the United States whose PII  
15 was compromised as a result of the data breach publicized in November  
16 2014.

### 17 **California Class**

18 All current and former SPE employees who reside or have resided in  
19 California and whose PII was compromised as a result of the data breach  
20 publicized in November 2014.

### 21 **Virginia Class**

22 All current and former SPE employees who reside or have resided in  
23 Virginia and whose PII was compromised as a result of the data breach  
24 publicized in November 2014.

### 25 **Colorado Class**

26 All current and former SPE employees who reside or have resided in  
27 Colorado and whose PII was compromised as a result of the data breach  
28 publicized in November 2014.

1           132. **Numerosity.** The proposed classes are sufficiently numerous, as  
2 thousands of current and former SPE employees have had their PII compromised.  
3  
4 The class members are so numerous and dispersed throughout the United States that  
5 joinder of all members is impracticable. Class members can be readily identified by  
6 records maintained by SPE.  
7

8           133. **Commonality.** Common questions of fact and law exist for each cause  
9 of action and predominate over questions affecting only individual class members.

10           For the Nationwide Class, common questions include:

- 11
- 12           a. Whether SPE had a legal duty to use reasonable security measures  
13           to protect class members' PII;
  - 14           b. Whether SPE timely, accurately, and adequately informed class  
15           members that their PII had been compromised;
  - 16           c. Whether SPE breached its legal duty by failing to protect class  
17           members' PII;
  - 18           d. Whether SPE acted reasonably in securing class members' PII;
  - 19           e. Whether class members are entitled to actual damages and/or  
20           statutory damages; and
  - 21           f. Whether class members are entitled to injunctive relief.

22

23

24

25           For the California Class, common questions include:

- 26           a. Whether SPE violated Civil Code section 1798.81.5 by failing to  
27           implement reasonable security procedures and practices;  
28

- 1           b. Whether SPE violated Civil Code section 1798.82 by failing to  
2 promptly notify class members that their personal information had  
3 been compromised;  
4  
5           c. Whether the information stolen in the Data Breach was “personal  
6 information” as defined by Civil Code sections 1798.80(e) and  
7 1798.81.5(d);  
8  
9           d. Whether class members are entitled to damages; and  
10  
11           e. Whether class members are entitled to injunctive relief.

12 For the Virginia Class, common questions include:

- 13           a. Whether SPE violated Virginia Code Annotated section 18.2-  
14 186.6(B) by failing to promptly notify class members that their  
15 personal information had been compromised;  
16  
17           b. Whether the information compromised by the Data Breach was  
18 “personal information” as defined by section 18.2-186.6(A);  
19  
20           c. Whether class members are entitled to damages; and  
21  
22           d. Whether class members are entitled to injunctive relief.

23 For the Colorado Class, common questions include:

- 24           a. Whether SPE violated Colorado Revised Statutes Annotated  
25 section 6-1-716(2) by failing to promptly notify class members  
26 that their personal information had been compromised;  
27  
28

- 1           b.     Whether the information compromised by the Data Breach  
2                     constituted “personal information” as defined by section 6-1-  
3                     716(1)(d);  
4  
5           c.     Whether class members are entitled to damages; and  
6  
7           d.     Whether class members are entitled to injunctive relief.

8           134. **Typicality.** Plaintiffs’ claims are typical of the claims of members of  
9 the proposed classes because, among other things, Plaintiffs and class members  
10 sustained similar injuries as a result of SPE’s uniform wrongful conduct and their  
11 legal claims all arise from the same conduct by SPE.  
12

13           135. **Adequacy.** Plaintiffs will fairly and adequately protect the interests of  
14 the proposed classes. Their interests do not conflict with class members’ interests  
15 and they have retained counsel experienced in complex class action and data privacy  
16 litigation to prosecute this case on behalf of the classes.  
17

18           136. **Rule 23(b)(3).** In addition to satisfying the prerequisites of Rule 23(a),  
19 Plaintiffs satisfy the requirements for maintaining a class action under Rule 23(b)(3).  
20 Common questions of law and fact predominate over any questions affecting only  
21 individual class members and a class action is superior to individual litigation. The  
22 amount of damages available to individual plaintiffs is insufficient to make litigation  
23 addressing SPE’s conduct economically feasible in the absence of the class action  
24 procedure. Individualized litigation also presents a potential for inconsistent or  
25 contradictory judgments, and increases the delay and expense to all parties and the  
26  
27  
28

1 court system presented by the legal and factual issues of the case. By contrast, the  
2 class action device presents far fewer management difficulties and provides the  
3 benefits of a single adjudication, economy of scale, and comprehensive supervision  
4 by a single court.  
5

6 137. **Rule 23(b)(2).** Plaintiffs also satisfy the requirements for maintaining a  
7 class action under Rule 23(b)(2). SPE has acted or refused to act on grounds that  
8 apply generally to the proposed classes, making final declaratory or injunctive relief  
9 appropriate with respect to the proposed classes as a whole.  
10

11 138. **Rule 23(c)(4).** Plaintiffs also satisfy the requirements for maintaining a  
12 class action under Rule 23(c)(4). The claims of class members are composed of  
13 particular issues that are common to all class members and capable of class wide  
14 resolution that will significantly advance the litigation.  
15  
16

## 17 **VIII. CAUSES OF ACTION**

### 18 **COUNT I: Negligence**

19 139. Plaintiffs reallege and incorporate by reference the allegations contained  
20 in each of the preceding paragraphs as if fully set forth herein.  
21

22 140. Plaintiffs bring this cause of action on behalf of the Nationwide Class.  
23

24 141. In collecting the financial, medical and other personal information of its  
25 employees, SPE as an employer owed Plaintiffs and class members a duty to exercise  
26 reasonable care in safeguarding and protecting that information. This duty included,  
27 among other things, maintaining and testing SPE's security systems and taking other  
28

1 reasonable security measures to protect and adequately secure the PII of Plaintiffs and  
2 class members from unauthorized access.

3  
4 142. SPE's security system and procedures for handling the financial, medical  
5 and other personal information of its current and former employees were intended to  
6 and did affect Plaintiffs and class members. SPE knew that by collecting and storing  
7 its employees' sensitive personal, financial and medical information, it undertook a  
8 responsibility to take reasonable security measures to protect the information from  
9 being stolen and exposed to unauthorized persons.

10  
11  
12 143. SPE owed a duty of care to Plaintiffs and class members because they  
13 were foreseeable and probable victims of any inadequate security practices. It was  
14 foreseeable that if SPE did not take reasonable security measures, the PII of Plaintiffs  
15 and members of the class would be stolen. Major corporations like SPE face a higher  
16 threat of security breaches than smaller companies due in part to the large amounts of  
17 data they possess. SPE knew or should have known its security systems were  
18 inadequate, particularly in light of the prior data breaches that SPE and its sister  
19 companies have experienced, and yet SPE failed to take reasonable precautions to  
20 safeguard the PII of its current and former employees.

21  
22  
23  
24 144. The duty SPE owed to Plaintiffs and members of the class to protect  
25 their PII is also underscored by the California Customer Records Act, the  
26 Confidentiality of Medical Information Act and Health Insurance Portability and  
27 Accountability Act ("HIPAA"), which recognize the importance of maintaining the  
28

1 confidentiality of personal and medical information and were enacted to protect  
2 individuals from the unauthorized exposure of their personal and medical  
3 information.  
4

5 145. SPE also had a duty to timely disclose to Plaintiffs and class members  
6 that their personal information had been or was reasonably believed to have been  
7 compromised. Timely disclosure was necessary so that Plaintiffs and members of the  
8 class could, among other things: (i) buy identity protection, monitoring, and recovery  
9 services; (ii) flag asset, credit, and tax accounts for fraud, including reporting the theft  
10 of their Social Security numbers to financial institutions, credit agencies, and the  
11 Internal Revenue Service; (iii) purchase or otherwise obtain credit reports; (iv)  
12 monitor credit, financial, utility, explanation of benefits, and other account statements  
13 on a monthly basis for unrecognized credit inquiries, Social Security numbers, home  
14 addresses, charges, and/or medical services; (v) place and renew credit fraud alerts on  
15 a quarterly basis; (vi) routinely monitor public records, loan data, or criminal records;  
16 (vii) contest fraudulent charges and other forms of criminal, financial and medical  
17 identity theft, and repair damage to credit and other financial accounts; and (viii) take  
18 other steps to protect themselves and recover from identity theft and fraud.  
19

20 146. SPE has admitted that its current and former employees' PII was  
21 exposed as a result of the Data Breach. As a result of SPE's negligence, Plaintiffs  
22 and members of the class have suffered and will suffer injury, including but not  
23 necessarily limited to: (1) the loss of the opportunity to control how their PII is used;  
24  
25  
26  
27  
28



1 (2) the diminution in the value and/or use of their PII entrusted to SPE for the purpose  
2 of deriving employment from SPE and with the understanding that SPE would  
3 safeguard their PII against theft and not allow access and misuse of their PII by  
4 others; (3) the compromise, publication, and/or theft of their PII and the PII of their  
5 family members and designated beneficiaries of employment-related benefits through  
6 SPE; (4) out-of-pocket costs associated with the prevention, detection, and recovery  
7 from identity theft and/or unauthorized use of financial and medical accounts; (5) lost  
8 opportunity costs associated with effort expended and the loss of productivity from  
9 addressing and attempting to mitigate the actual and future consequences of the  
10 breach, including but not limited to efforts spent researching how to prevent, detect,  
11 contest and recover from identity and health care/medical data misuse; (6) costs  
12 associated with the ability to use credit and assets frozen or flagged due to credit  
13 misuse, including complete credit denial and/or increased costs to use credit, credit  
14 scores, credit reports and assets; (7) unauthorized use of compromised PII to open  
15 new financial and/or health care or medical accounts; (8) tax fraud and/or other  
16 unauthorized charges to financial, health care or medical accounts and associated lack  
17 of access to funds while proper information is confirmed and corrected; (9) the  
18 continued risk to their PII, and the PII of their family members and designated  
19 beneficiaries of employment-related benefits through SPE, which remain in SPE's  
20 possession and are subject to further breaches so long as SPE fails to undertake  
21 appropriate and adequate measures to protect the PII in its possession; and (10) future  
22  
23  
24  
25  
26  
27  
28

1 costs in terms of time, effort and money that will be expended, to prevent, detect,  
2 contest, and repair the impact of the PII compromised as a result of the Data Breach  
3  
4 for the remainder of the lives of the Nationwide Class members, their families, and  
5 their designated beneficiaries of employment-related benefits through SPE.

6 147. There is a very close connection between SPE's failure to employ  
7 reasonable security protections of its current and former employees' PII and the  
8 injuries suffered by Plaintiffs and class members. When individuals have their PII  
9 stolen, they are at risk for identity theft, and need to: (i) buy identity protection,  
10 monitoring, and recovery services; (ii) flag asset, credit, and tax accounts for fraud,  
11 including reporting the theft of their Social Security numbers to financial institutions,  
12 credit agencies, and the Internal Revenue Service; (iii) purchase or otherwise obtain  
13 credit reports; (iv) monitor credit, financial, utility, explanation of benefits, and other  
14 account statements on a monthly basis for unrecognized credit inquiries, Social  
15 Security numbers, home addresses, charges, and/or medical services; (v) place and  
16 renew credit fraud alerts on a quarterly basis; (vi) routinely monitor public records,  
17 loan data, or criminal records; (vii) contest fraudulent charges and other forms of  
18 criminal, financial and medical identity theft, and repair damage to credit and other  
19 financial accounts; and (viii) take other steps to protect themselves and recover from  
20 identity theft and fraud.

21  
22  
23  
24  
25  
26 148. SPE is responsible for not protecting the PII of its current and former  
27 employees. If SPE had reasonable security measures in place, data thieves would not  
28

1 have been able to steal and expose the PII of thousands of current and former SPE  
2 employees.

3  
4 149. The policy of preventing future harm weighs strongly in favor of finding  
5 a special relationship between SPE and its current and former employees. SPE's  
6 employees were required to share sensitive personal and medical information with  
7 SPE as a condition of employment and depended on SPE as their employer to ensure  
8 that this information is protected from theft and unauthorized disclosure. If  
9 companies are not held accountable for failing to take reasonable security measures to  
10 protect their employees' PII, they will not take the steps that are necessary to protect  
11 against future data breaches.  
12

13  
14 150. SPE breached its duty to exercise reasonable care in protecting the PII of  
15 Plaintiffs and the class by failing to implement and maintain adequate security  
16 measures to safeguard its employees' PII, failing to monitor its systems to identify  
17 suspicious activity, and allowing unauthorized access to the PII of Plaintiffs and class  
18 members.  
19

20  
21 151. SPE breached its duty to timely notify Plaintiffs and the class about the  
22 Data Breach. SPE waited several days after discovering the Data Breach to inform its  
23 current employees that their PII had been or was reasonably believed to have been  
24 compromised, and waited even longer to issue a notice to its former employees  
25 affected by the breach. SPE has yet to notify some former employees.  
26  
27  
28

1           152. But for SPE's failure to implement and maintain adequate security  
2 measures to protect its employees' PII and failure to monitor its systems to identify  
3 suspicious activity, the PII of Plaintiffs and class members would not have been  
4 stolen, Plaintiffs and class members would not have been injured, and Plaintiffs and  
5 class members would not be at a heightened risk of identity theft in the future.  
6

7  
8           153. SPE's negligence was a substantial factor in causing harm to Plaintiffs  
9 and class members. As a direct and proximate result of SPE's failure to exercise  
10 reasonable care and use commercially reasonable security measures, the PII of SPE's  
11 current and former employees was accessed by unauthorized individuals who: (i)  
12 have already used the compromised information to commit identity theft and fraud;  
13 (ii) can continue to use this compromised PII to commit identity theft and identity and  
14 health care and/or medical fraud; and (iii) have posted the information on the internet,  
15 allowing themselves and others to commit identity theft, and identity and health care  
16 and/or medical fraud using the compromised PII indefinitely.  
17  
18

19  
20           154. As a result of SPE's negligence, Plaintiffs and members of the class are  
21 entitled to injunctive relief, including, but not limited to an order that SPE: (1) engage  
22 third party security auditors/penetration testers as well as internal security personnel  
23 to conduct testing consistent with prudent industry practices, including simulated  
24 attacks, penetration tests, and audits on SPE's systems on a periodic basis; (2) engage  
25 third party security auditors and internal personnel to run automated security  
26 monitoring consistent with prudent industry practices; (3) audit, test, and train its  
27  
28

1 security personnel regarding any new or modified procedures; (4) purge, delete and  
2 destroy, in a secure manner, employee data not necessary for its business operations;  
3  
4 (5) conduct regular database scanning and securing checks consistent with prudent  
5 industry practices; (6) periodically conduct internal training and education to inform  
6 internal security personnel how to identify and contain a breach when it occurs and  
7 what to do in response to a breach consistent with prudent industry practices; (7)  
8 receive periodic compliance audits by a third party regarding the security of the  
9 computer systems SPE uses to store the personal information of its current and  
10 former employees; (8) meaningfully educate its current and former employees about  
11 the threats they face as a result of the loss of their PII to third parties, as well as the  
12 steps they must take to protect themselves; and (9) provide ongoing identity theft  
13 protection, monitoring, and recovery services to Plaintiffs and class members, as well  
14 as their dependents and designated beneficiaries of employment-related benefits  
15 through SPE.

16  
17  
18  
19  
20 155. Plaintiffs and the class are also entitled to damages and reasonable  
21 attorneys' fees and costs. Plaintiffs also seek reasonable attorneys' fees and costs  
22 under applicable law including Federal Rule of Civil Procedure 23 and California  
23 Code of Civil Procedure § 1021.5.

24  
25 **COUNT II: Breach of Implied Contract**

26  
27 156. Plaintiffs reallege and incorporate by reference the allegations contained  
28 in each of the preceding paragraphs as if fully set forth herein.

1 157. Plaintiffs bring this cause of action on behalf of the Nationwide Class.

2 158. SPE offered employment to Plaintiffs and class members in exchange  
3  
4 for compensation and other employment benefits. To receive compensation and other  
5 employment benefits, SPE required Plaintiffs and class members to provide their PII,  
6 including names, addresses, Social Security numbers, medical information, and other  
7 personal information.  
8

9 159. SPE had an implied duty of good faith to ensure that the PII of Plaintiffs  
10 and class members in its possession was only used to provide the agreed-upon  
11 compensation and other employment benefits from SPE.  
12

13 160. SPE was therefore required to reasonably safeguard and protect the PII  
14 of Plaintiffs and class members from unauthorized uses, and to timely and accurately  
15 notify Plaintiffs and class members if their PII was compromised so that Plaintiffs  
16 and class members could act to mitigate the harm caused by the loss of opportunity to  
17 control how their PII was used.  
18

19 161. Plaintiffs and class members accepted SPE's employment offer and fully  
20 performed their obligations under the implied contract with SPE by providing their  
21 PII to SPE, among other obligations.  
22

23 162. Plaintiffs and class members would not have provided and entrusted  
24 their PII to SPE in the absence of their implied contracts with SPE, and would have  
25 instead retained the opportunity to control their PII for uses other than compensation  
26 and other employment benefits from SPE.  
27  
28

1           163. SPE breached the implied contracts with Plaintiffs and class members by  
2 failing to reasonably safeguard and protect Plaintiffs' and class members' PII and by  
3 failing to provide timely and accurate notice to Plaintiffs and class members that their  
4 PII was compromised as a result of the Data Breach.  
5

6           164. As a proximate and direct result of SPE's breaches of its implied  
7 contracts with Plaintiffs and class members, Plaintiffs and class members have  
8 suffered and will suffer injury, including but not necessarily limited to: (1) the loss of  
9 the opportunity to control how their PII is used; (2) the diminution in the value and/or  
10 use of their PII entrusted to SPE for the purpose of deriving employment from SPE  
11 and with the understanding that SPE would safeguard their PII against theft and not  
12 allow access and misuse of their PII by others; (3) the compromise, publication,  
13 and/or theft of their PII and the PII of their family members and designated  
14 beneficiaries of employment-related benefits through SPE; (4) out-of-pocket costs  
15 associated with the prevention, detection, and recovery from identity theft and/or  
16 unauthorized use of financial and medical accounts; (5) lost opportunity costs  
17 associated with effort expended and the loss of productivity addressing and  
18 attempting to mitigate the actual and future consequences of the breach, including but  
19 not limited to efforts spent researching how to prevent, detect, contest and recover  
20 from identity and health care/medical data misuse; (6) costs associated with the  
21 ability to use credit and assets frozen or flagged due to credit misuse, including  
22 complete credit denial and/or increased costs to use credit, credit scores, credit reports  
23  
24  
25  
26  
27  
28

1 and assets; (7) unauthorized use of compromised PII to open new financial and/or  
2 health care or medical accounts; (8) tax fraud and/or other unauthorized charges to  
3 financial, health care or medical accounts and associated lack of access to funds while  
4 proper information is confirmed and corrected; (9) the continued risk to their PII, and  
5 the PII of their family members and designated beneficiaries of employment-related  
6 benefits through SPE, which remain in SPE’s possession and are subject to further  
7 breaches so long as SPE fails to undertake appropriate and adequate measures to  
8 protect the PII in its possession; and (10) future costs in terms of time, effort and  
9 money that will be expended, to prevent, detect, contest, and repair the impact of the  
10 PII compromised as a result of the Data Breach for the remainder of the lives of the  
11 Nationwide Class members, their families, and their designated beneficiaries of  
12 employment-related benefits through SPE.  
13  
14  
15  
16

17 **COUNT III: Violation of the California Customer Records Act**  
18 **California Civil Code Section 1798.80 *et seq.***

19 165. Plaintiffs reallege and incorporate by reference the allegations contained  
20 in each of the preceding paragraphs as if fully set forth herein.  
21

22 166. Plaintiffs bring this cause of action on behalf of the California Class.

23 167. The California Legislature enacted Civil Code section 1798.81.5 “to  
24 ensure that personal information about California residents is protected.” The statute  
25 requires that any business that “owns, licenses, or maintains personal information  
26 about a California resident ... implement and maintain reasonable security procedures  
27  
28



1 and practices appropriate to the nature of the information, to protect the personal  
2 information from unauthorized access, destruction, use, modification, or disclosure.”  
3

4 168. SPE is a “business” as defined by Civil Code section 1798.80(a).

5 169. Each Plaintiff and member of the class is an “individual” as defined by  
6 Civil Code section 1798.80(d).  
7

8 170. The employee information taken in the Data Breach was “personal  
9 information” as defined by Civil Code sections 1798.80(e) and 1798.81.5(d), which  
10 includes “information that identifies, relates to, describes, or is capable of being  
11 associated with, a particular individual, including, but not limited to, his or her name,  
12 signature, Social Security number, physical characteristics or description, address,  
13 telephone number, passport number, driver’s license or state identification card  
14 number, insurance policy number, education, employment, employment history, bank  
15 account number, credit card number, debit card number, or any other financial  
16 information, medical information, or health insurance information.”  
17  
18  
19

20 171. The breach of the personal information of thousands of current and  
21 former SPE employees was a “breach of the security system” of SPE as defined by  
22 Civil Code section 1798.82(g).  
23

24 172. By failing to implement reasonable security measures appropriate to the  
25 nature of the personal information of its current and former employees, SPE violated  
26 Civil Code section 1798.81.5.  
27  
28

1           173. In addition, by failing to immediately notify all affected current and  
2 former SPE employees that their personal information had been acquired (or was  
3 reasonably believed to have been acquired) by unauthorized persons in the Data  
4 Breach, SPE violated Civil Code section 1798.82 of the same title. SPE's failure to  
5 immediately notify employees of the breach caused class members to suffer damages  
6 because they have lost the opportunity to immediately: (i) buy identity protection,  
7 monitoring, and recovery services; (ii) flag asset, credit, and tax accounts for fraud,  
8 including reporting the theft of their Social Security numbers to financial institutions,  
9 credit agencies, and the Internal Revenue Service; (iii) purchase or otherwise obtain  
10 credit reports; (iv) monitor credit, financial, utility, explanation of benefits, and other  
11 account statements on a monthly basis for unrecognized credit inquiries, Social  
12 Security numbers, home addresses, charges, and/or medical services; (v) place and  
13 renew credit fraud alerts on a quarterly basis; (vi) routinely monitor public records,  
14 loan data, or criminal records; (vii) contest fraudulent charges and other forms of  
15 criminal, financial and medical identity theft, and repair damage to credit and other  
16 financial accounts; and (viii) take other steps to protect themselves and recover from  
17 identity theft and fraud.  
18  
19  
20  
21  
22  
23

24           174. Because it violated Civil Code sections 1798.81.5 and 1798.82, SPE  
25 "may be enjoined" under Civil Code section 1798.84(e).  
26

27           175. Plaintiffs request that the Court enter an injunction requiring SPE to  
28 implement and maintain reasonable security procedures to protect its employees' PII,

1 including, but not limited to, ordering that SPE: (1) engage third party security  
2 auditors/penetration testers as well as internal security personnel to conduct testing  
3 consistent with prudent industry practices, including simulated attacks, penetration  
4 tests, and audits on SPE's systems on a periodic basis; (2) engage third party security  
5 auditors and internal personnel to run automated security monitoring consistent with  
6 prudent industry practices; (3) audit, test, and train its security personnel regarding  
7 any new or modified procedures; (4) purge, delete and destroy, in a secure manner,  
8 employee data not necessary for its business operations; (5) conduct regular database  
9 scanning and securing checks consistent with prudent industry practices; (6)  
10 periodically conduct internal training and education to inform internal security  
11 personnel how to identify and contain a breach when it occurs and what to do in  
12 response to a breach consistent with prudent industry practices; (7) receive periodic  
13 compliance audits by a third party regarding the security of the computer systems  
14 SPE uses to store the personal information of its current and former employees; (8)  
15 meaningfully educate its current and former employees about the threats they face as  
16 a result of the loss of their PII to third parties, as well as the steps they must take to  
17 protect themselves; and (9) provide ongoing identity theft protection, monitoring, and  
18 recovery services to Plaintiffs and class members, as well as their dependents and  
19 designated beneficiaries of employment-related benefits through SPE.  
20  
21  
22  
23  
24  
25

26 176. Plaintiffs further request that the Court order SPE to (1) identify and  
27 notify all members of the class who have not yet been informed of the Data Breach;  
28

1 and (2) notify affected current and former employees of any future data breaches by  
2 email within 24 hours of SPE's discovery of a breach or possible breach and by mail  
3 within 72 hours.  
4

5 177. As a result of SPE's violations of Civil Code sections 1798.81.5 and  
6 1798.82, Plaintiffs and members of the California Class have incurred and will incur  
7 damages, including but not necessarily limited to: (1) the loss of the opportunity to  
8 control how their PII is used; (2) the diminution in the value and/or use of their PII  
9 entrusted to SPE for the purpose of deriving employment from SPE and with the  
10 understanding that SPE would safeguard their PII against theft and not allow access  
11 and misuse of their PII by others; (3) the compromise, publication, and/or theft of  
12 their PII and the PII of their family members and designated beneficiaries of  
13 employment-related benefits through SPE; (4) out-of-pocket costs associated with the  
14 prevention, detection, and recovery from identity theft and/or unauthorized use of  
15 financial and medical accounts; (5) lost opportunity costs associated with effort  
16 expended and the loss of productivity from addressing and attempting to mitigate the  
17 actual and future consequences of the breach, including but not limited to efforts  
18 spent researching how to prevent, detect, contest and recover from identity and health  
19 care/medical data misuse; (6) costs associated with the ability to use credit and assets  
20 frozen or flagged due to credit misuse, including complete credit denial and/or  
21 increased costs to use credit, credit scores, credit reports and assets; (7) unauthorized  
22 use of compromised PII to open new financial and/or health care or medical accounts;  
23  
24  
25  
26  
27  
28

1 (8) tax fraud and/or other unauthorized charges to financial, health care or medical  
2 accounts and associated lack of access to funds while proper information is confirmed  
3 and corrected; (9) the continued risk to their PII, and the PII of their family members  
4 and designated beneficiaries of employment-related benefits through SPE, which  
5 remain in SPE's possession and are subject to further breaches so long as SPE fails to  
6 undertake appropriate and adequate measures to protect the PII in its possession; and  
7  
8 (10) future costs in terms of time, effort and money that will be expended, to prevent,  
9 detect, contest, and repair the impact of the PII compromised as a result of the Data  
10 Breach for the remainder of the lives of the California Class members, their families,  
11 and their designated beneficiaries of employment-related benefits through SPE.  
12  
13

14 178. Plaintiffs seek all remedies available under Civil Code section 1798.84,  
15 including actual and statutory damages, equitable relief, and reasonable attorneys'  
16 fees. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law  
17 including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure  
18 § 1021.5.  
19  
20

21 **COUNT IV: Violation of California Confidentiality of Medical Information Act**  
22 **California Civil Code § 56 *et seq.***

23 179. Plaintiffs reallege and incorporate by reference the allegations contained  
24 in each of the preceding paragraphs as if fully set forth herein.  
25

26 180. Plaintiffs bring this cause of action on behalf of the Nationwide Class.

27 181. California's Confidentiality of Medical Information Act ("CMIA"), Cal.  
28 Civ. Code § 56, *et seq.*, requires employers like SPE to protect their employees'

1 confidential medical information and not release private medical information without  
2 signed proper authorization.  
3

4 182. The CMIA defines “medical information” as “any individually  
5 identifiable information, in electronic or physical form, in possession of or derived  
6 from a provider of health care, health care service plan, pharmaceutical company, or  
7 contractor regarding a patient’s medical history, mental or physical condition, or  
8 treatment.” The CMIA defines “individually identifiable” as “medical information  
9 [that] includes or contains any element of personal identifying information sufficient  
10 to allow identification of the individual, such as the patient’s name, address,  
11 electronic mail address, telephone number, or Social Security number, or other  
12 information that, alone or in combination with other publicly available information,  
13 reveals the individual's identity.”  
14  
15  
16

17 183. SPE has violated section 56.20(a) of the CMIA, which requires an  
18 “employer who receives medical information [to] establish appropriate procedures to  
19 ensure the confidentiality and protection from unauthorized use and disclosure of that  
20 information.” The procedures the employer must establish “may include, but are not  
21 limited to, instruction regarding confidentiality of employees and agents handling  
22 files containing medical information, and security systems restricting access to files  
23 containing medical information.” SPE violated section 56.20(a) of the CMIA by  
24 failing to maintain the confidentiality of class members’ medical information and by  
25  
26  
27  
28

1 failing to institute reasonable safeguards to protect their medical information from  
2 disclosure.

3  
4 184. SPE also violated section 56.36(b) of the CMIA by negligently releasing  
5 Plaintiffs' and class members' medical information.

6  
7 185. SPE did not obtain Plaintiffs' or class members' written authorization to  
8 disclose or release their medical information.

9  
10 186. As a result of the Data Breach, class members' medical information has  
11 been posted to the internet where it has been viewed by members of the media and  
12 the public. This medical information includes complaints from employees about  
13 unpaid medical insurance claims, spreadsheets that contained the health conditions  
14 and medical procedures for employees for diagnoses such as cancer, heart disorders,  
15 and end-stage renal disease, along with employees' PII that was contained in the  
16 spreadsheets and other data released in the breach.

17  
18 187. SPE has admitted that the personal information exposed by the Data  
19 Breach included "HIPAA protected health information, such as name, Social Security  
20 number, claims appeals information you submitted to SPE (including diagnosis and  
21 disability code), date of birth, home address, and member ID number to the extent  
22 that you and/or your dependents participated in SPE health plans," as well as  
23 "health/medical information that [employees] provided to [SPE] outside of SPE  
24 health plans."  
25  
26  
27  
28

1           188. Among other things, SPE is and was negligent in failing to maintain its  
2 current and former employees' medical information in encrypted form; failing to use  
3 reasonable security procedures to prevent unauthorized access to files containing the  
4 medical information; failing to use reasonable authentication procedures so that the  
5 medical information could be tracked in case of a security breach; delaying notifying  
6 its current and former employees that their private medical information had been  
7 compromised; and allowing unauthorized access to employees' private medical files,  
8 all in violation of the CMIA and HIPAA.  
9  
10

11  
12           189. Plaintiffs request that the Court enter an injunction requiring SPE to  
13 implement and maintain reasonable security procedures to protect its employees'  
14 medical information in compliance with the CMIA, including, but not limited to,  
15 ordering that SPE: (1) engage third party security auditors/penetration testers as well  
16 as internal security personnel to conduct testing consistent with prudent industry  
17 practices, including simulated attacks, penetration tests, and audits on SPE's systems  
18 on a periodic basis; (2) engage third party security auditors and internal personnel,  
19 consistent with prudent industry practices, to run automated security monitoring –  
20 particularly for employees' medical information – consistent with prudent industry  
21 practices; (3) audit, test, and train its security personnel regarding any new or  
22 modified procedures designed to protect employees' medical information; (4) purge,  
23 delete and destroy, in a secure manner, employees' medical information not  
24 necessary for its business operations; (5) conduct regular database scanning and  
25  
26  
27  
28



1 securing checks, consistent with prudent industry practices; (6) periodically conduct  
2 internal training and education to inform internal security personnel how to identify  
3 and contain a breach when it occurs and what to do in response to a breach, consistent  
4 with prudent industry practices; (7) receive periodic compliance audits by a third  
5 party regarding the security of the computer systems SPE uses to store the personal  
6 information of its current and former employees; (8) meaningfully educate its current  
7 and former employees about the threats they face as a result of the loss of their  
8 personal information to third parties, as well as the steps they must take to protect  
9 themselves; and (9) provide ongoing identity theft protection, monitoring, and  
10 recovery services to Plaintiffs and class members, as well as their dependents and  
11 designated beneficiaries of employment-related benefits through SPE.  
12

13  
14  
15  
16 190. Plaintiffs also seek an award of \$1,000 in statutory damages for each  
17 class member pursuant to section 56.36(b)(1) of the CMIA. An award of statutory  
18 damages is necessary to deter future violations by SPE and other employers.  
19

20 191. Plaintiffs also seek actual damages pursuant to section 56.36(b)(2). As a  
21 result of SPE's violation of the CMIA, Plaintiffs and class members have incurred  
22 and will incur damages, including but not necessarily limited to: (1) the loss of the  
23 opportunity to control how their PII is used; (2) the diminution in the value and/or use  
24 of their PII entrusted to SPE for the purpose of deriving employment from SPE and  
25 with the understanding that SPE would safeguard their PII against theft and not allow  
26 access and misuse of their PII by others; (3) the compromise, publication, and/or theft  
27  
28

1 of their PII and the PII of their family members and designated beneficiaries of  
2 employment-related benefits through SPE; (4) out-of-pocket costs associated with the  
3 prevention, detection, and recovery from identity theft and/or unauthorized use of  
4 financial and medical accounts; (5) lost opportunity costs associated with effort  
5 expended and the loss of productivity from addressing and attempting to mitigate the  
6 actual and future consequences of the breach, including but not limited to efforts  
7 spent researching how to prevent, detect, contest and recover from identity and health  
8 care/medical data misuse; (6) costs associated with the ability to use credit and assets  
9 frozen or flagged due to credit misuse, including complete credit denial and/or  
10 increased costs to use credit, credit scores, credit reports and assets; (7) unauthorized  
11 use of compromised PII to open new financial and/or health care or medical accounts;  
12 (8) tax fraud and/or other unauthorized charges to financial, health care or medical  
13 accounts and associated lack of access to funds while proper information is confirmed  
14 and corrected; (9) the continued risk to their PII, and the PII of their family members  
15 and designated beneficiaries of employment-related benefits through SPE, which  
16 remain in SPE's possession and are subject to further breaches so long as SPE fails to  
17 undertake appropriate and adequate measures to protect the PII in its possession; and  
18 (10) future costs in terms of time, effort and money that will be expended, to prevent,  
19 detect, contest, and repair the impact of the PII compromised as a result of the Data  
20 Breach for the remainder of the lives of the Nationwide Class members, their  
21  
22  
23  
24  
25  
26  
27  
28

1 families, and their designated beneficiaries of employment-related benefits through  
2 SPE.  
3

4 192. Plaintiffs also seek reasonable attorneys' fees and costs under applicable  
5 law including Federal Rule of Civil Procedure 23 and California Code of Civil  
6 Procedure § 1021.5.  
7

8 **COUNT V: Violation of the Unfair Competition Law**  
9 **California Business and Professions Code Section 17200 *et seq.***

10 193. Plaintiffs reallege and incorporate by reference the allegations contained  
11 in each of the preceding paragraphs as if fully set forth herein.  
12

13 194. Plaintiffs bring this cause of action on behalf of the Nationwide Class.

14 195. SPE engaged in unlawful, unfair, and fraudulent business practices in  
15 violation of the Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.*  
16 (“UCL”).  
17

18 196. SPE's acts, omissions and conduct constitute unlawful, unfair, and  
19 fraudulent business practices under the UCL.  
20

21 197. SPE's acts, omissions and conduct were unlawful because they violated  
22 the California Customer Records Act, the CMIA, and HIPAA, and because they were  
23 negligent.  
24

25 198. SPE's practices were unlawful and in violation of Civil Code section  
26 1798.81.5(b) because SPE failed to take reasonable security measures in protecting  
27 its current and former employees' PII.  
28

1           199. SPE's practices were also unlawful and in violation of California Civil  
2 Code section 1798.82 because SPE unreasonably delayed informing Plaintiffs and  
3 class members about the breach of security after SPE knew the Data Breach occurred.  
4

5           200. SPE's practices were unlawful and in violation of section 56.20 of the  
6 CMIA because it did not establish proper procedures to secure the confidentiality of  
7 its current and former employees' medical information.  
8

9           201. SPE's practices were also unlawful and in violation of section 56.36(b)  
10 of the CMIA because SPE negligently released Plaintiffs' and class members'  
11 medical information that was within SPE's control.  
12

13           202. SPE's practices were also unlawful and in violation of HIPAA because  
14 SPE failed to establish procedures to keep employees' medical information  
15 confidential and private.  
16

17           203. SPE's acts, omissions and conduct constitute a violation of the unlawful  
18 prong of the UCL because SPE failed to comport with a reasonable standard of care  
19 and public policy as reflected in statutes like the Information Practices Act of 1977,  
20 HIPAA, the CMIA, and the California Customer Records Act, which were enacted to  
21 protect individuals' personal information and ensure that entities that solicit or are  
22 entrusted with personal information use reasonable security measures.  
23  
24

25           204. In unduly delaying informing Plaintiffs and the class members of the  
26 Data Breach, SPE engaged in unfair business practices by engaging in conduct that  
27 undermines or violates the stated policies underlying the California Customer  
28

1 Records Act and other privacy statutes. In enacting the California Customer Records  
2 Act, the Legislature stated that “[i]dentity theft is costly to the marketplace and to  
3 consumers” and that “victims of identity theft must act quickly to minimize the  
4 damage; therefore expeditious notification of possible misuse of a person’s personal  
5 information is imperative.” 2002 Cal. Legis. Serv. Ch. 1054 (A.B. 700) (WEST).  
6  
7 SPE’s conduct also undermines California public policy as reflected in other statutes  
8 such as the Information Practices Act of 1977, which was enacted to protect  
9 individuals’ data and ensure that entities who solicit or are entrusted with personal  
10 data use reasonable security measures.  
11  
12

13 205. SPE’s acts, omissions, and conduct also constitute “unfair” business acts  
14 or practices because they offend public policy and constitute immoral, unethical, and  
15 unscrupulous activities that caused substantial injury, including to Plaintiffs and class  
16 members. The gravity of harm resulting from SPE’s conduct outweighs any potential  
17 benefits attributable to the conduct and there were reasonably available alternatives to  
18 further SPE’s legitimate business interests. SPE’s conduct also undermines public  
19 policy as reflected in statutes like the Information Practices Act of 1977, Cal. Civ.  
20 Code § 1798, *et seq.*, HIPAA, the CMIA, and the California Customer Records Act,  
21 which were enacted to protect individuals’ personal data and ensure that entities who  
22 solicit or are entrusted with personal data use reasonable security measures.  
23  
24  
25

26 206. SPE has engaged in fraudulent business practices by making material  
27 misrepresentations and by failing to disclose material information regarding SPE’s  
28

1 deficient security policies and practices, the security of the PII of Plaintiffs and class  
2 members, and the Data Breach.

3  
4 207. SPE had exclusive knowledge of material information regarding its  
5 deficient security policies and practices, and regarding the security of the PII of  
6 Plaintiffs and class members. This exclusive knowledge includes, but is not limited  
7 to, information that SPE received through internal and other non-public audits and  
8 reviews that concluded that SPE's security policies were substandard and deficient,  
9 and that the PII of Plaintiffs and class members and other SPE data was vulnerable as  
10 a result. This exclusive knowledge also includes information regarding SPE's data  
11 security, not reported publicly, that SPE received in connection with data breaches at  
12 SPE and other Sony companies that occurred over the years. SPE also had exclusive  
13 knowledge concerning the measures, or lack thereof, that SPE took in response to the  
14 data breaches that have occurred over the years at SPE and other Sony companies and  
15 in response to the various audits that have reflected security gaps at SPE and other  
16 Sony companies.

17  
18 208. SPE also had exclusive knowledge about the extent of the Data Breach,  
19 including during the days and weeks following the Data Breach.

20  
21 209. SPE also had exclusive knowledge about the length of time that it  
22 maintained former employees' PII after they left SPE's employment.

23  
24 210. SPE failed to disclose, and actively concealed, the material information  
25 it had regarding SPE's deficient security policies and practices, and regarding the  
26  
27  
28

1 security of the PII of Plaintiffs and class members. For example, even though SPE  
2 has long known, through internal audits and otherwise, that its security policies and  
3 practices were substandard and deficient, and that the PII of Plaintiffs and class  
4 members was vulnerable as a result, SPE failed to disclose this information to, and  
5 actively concealed this information from, Plaintiffs, class members and the public.  
6  
7 SPE also did not disclose, and actively concealed, information regarding the  
8 extensive length of time that it maintains former employees' PII and other records.  
9 Likewise, in the days and weeks following the Data Breach, SPE failed to disclose,  
10 and actively concealed, information that it had regarding the extent and nature of the  
11 Data Breach.  
12  
13

14           211. SPE also has made material affirmative misrepresentations about SPE's  
15 security policies and practices and the security of the PII of Plaintiffs and class  
16 members. For example, following the 2011 PSN data breach, Sony President Kazuo  
17 Hirai indicated that, after that breach, Sony had "basically ... done everything to  
18 bring our practices at least in line with industry standards or better." In fact, contrary  
19 to this representation, Sony failed to invest the resources necessary to bring the  
20 security practices at the Sony companies in line with industry standards.  
21  
22

23           212. SPE had a duty to disclose the material information that it had because,  
24 *inter alia*, it had exclusive knowledge of the information, it actively concealed the  
25 information, it made affirmative statements that were inconsistent with the  
26 information it did not disclose, and because SPE was in a fiduciary position vis-à-vis  
27  
28

1 Plaintiffs and class members by virtue of the fact that SPE collected and maintained  
2 their financial information, medical information, and other PII.  
3

4 213. SPE's misrepresentations and omissions were material, misleading, and  
5 had a tendency to deceive.

6 214. Plaintiffs were misled by SPE's misrepresentations and omissions about  
7 SPE's data security, and they reasonably relied upon them to their detriment. But for  
8 SPE's misrepresentations and omissions, Plaintiffs would not have provided the PII  
9 that they provided to SPE (regarding themselves and their family members) and  
10 would have insisted that their PII be more securely protected and removed from  
11 SPE's systems promptly after their employment ended. They also would have taken  
12 additional steps to protect their identities and to protect themselves from the sort of  
13 harm that could flow from SPE's lax security measures. But for SPE's  
14 misrepresentations and omissions, Plaintiffs would not be experiencing identity theft,  
15 identity fraud, and/or the increased risk of harm they are now facing, as a result of the  
16 Data Breach. But for the fact that SPE sat on information regarding the Data Breach,  
17 rather than immediately disclosing it, Plaintiffs would have taken more immediate  
18 steps to protect their identities and they would have been able to minimize the harm  
19 they have suffered as a result of the Data Breach.  
20  
21  
22  
23  
24

25 215. As a direct and proximate result of SPE's unlawful, unfair, and  
26 fraudulent business practices as alleged herein, Plaintiffs and members of the class  
27 have suffered injury in fact. Plaintiffs and the class have been injured in that their  
28



1 personal, financial, and medical PII has been compromised, subject to identity theft,  
2 identity fraud, and/or is at risk for future identity theft and fraudulent activity on their  
3 financial accounts. Class members have also lost money and property that would not  
4 have be lost but for SPE's unlawful and unfair conduct.  
5

6           216. As a direct and proximate result of SPE's unlawful, unfair, and  
7 fraudulent business practices as alleged herein, Plaintiffs and class members already  
8 suffer from identity theft, identity and financial fraud, and/or a continuing increased  
9 risk of identity theft and identity, financial and medical fraud due to the compromise,  
10 publication, and/or unauthorized use of their financial, health care, and/or medical  
11 PII. Plaintiffs have also been injured by, among other things: (1) the loss of the  
12 opportunity to control how their PII is used; (2) the diminution in the value and/or use  
13 of their PII entrusted to SPE for the purpose of deriving employment from SPE and  
14 with the understanding that SPE would safeguard their PII against theft and not allow  
15 access and misuse of their PII by others; (3) the compromise, publication, and/or theft  
16 of their PII and the PII of their family members and designated beneficiaries of  
17 employment-related benefits through SPE; (4) out-of-pocket costs associated with the  
18 prevention, detection, and recovery from identity theft and/or unauthorized use of  
19 financial and medical accounts; (5) lost opportunity costs associated with effort  
20 expended and the loss of productivity from addressing and attempting to mitigate the  
21 actual and future consequences of the breach, including but not limited to efforts  
22 spent researching how to prevent, detect, contest and recover from identity and health  
23  
24  
25  
26  
27  
28

1 care/medical data misuse; (6) costs associated with the ability to use credit and assets  
2 frozen or flagged due to credit misuse, including complete credit denial and/or  
3 increased costs to use credit, credit scores, credit reports and assets; (7) unauthorized  
4 use of compromised PII to open new financial and/or health care or medical accounts;  
5 (8) tax fraud and/or other unauthorized charges to financial, health care or medical  
6 accounts and associated lack of access to funds while proper information is confirmed  
7 and corrected; (9) the continued risk to their PII, and the PII of their family members  
8 and designated beneficiaries of employment-related benefits through SPE, which  
9 remain in SPE's possession and are subject to further breaches so long as SPE fails to  
10 undertake appropriate and adequate measures to protect the PII in its possession; and  
11 (10) future costs in terms of time, effort and money that will be expended, to prevent,  
12 detect, contest, and repair the impact of the PII compromised as a result of the Data  
13 Breach for the remainder of the lives of the Nationwide Class members, their  
14 families, and their designated beneficiaries of employment-related benefits through  
15 SPE.  
16  
17  
18  
19  
20

21 217. As a result of SPE's violations of the UCL, Plaintiffs and members of  
22 the class are entitled to injunctive relief, including, but not limited to an order that  
23 SPE: (1) engage third party security auditors/penetration testers as well as internal  
24 security personnel to conduct testing consistent with prudent industry practices,  
25 including simulated attacks, penetration tests, and audits on SPE's systems on a  
26 periodic basis; (2) engage third party security auditors and internal personnel to run  
27  
28

1 automated security monitoring consistent with prudent industry practices; (3) audit,  
2 test, and train its security personnel regarding any new or modified procedures; (4)  
3 purge, delete and destroy, in a secure manner, employee data not necessary for its  
4 business operations; (5) conduct regular database scanning and securing checks  
5 consistent with prudent industry practices; (6) periodically conduct internal training  
6 and education to inform internal security personnel how to identify and contain a  
7 breach when it occurs and what to do in response to a breach consistent with prudent  
8 industry practices; (7) receive periodic compliance audits by a third party regarding  
9 the security of the computer systems SPE uses to store the PII of its current and  
10 former employees; (8) meaningfully educate its current and former employees about  
11 the threats they face as a result of the loss of their PII to third parties, as well as the  
12 steps they must take to protect themselves; and (9) provide ongoing identity theft  
13 protection, monitoring, and recovery services, to Plaintiffs and class members, as  
14 well as their dependents and designated beneficiaries of employment-related benefits  
15 through SPE.

21 218. Because of SPE's unlawful, unfair, and fraudulent business practices,  
22 Plaintiffs and the class are entitled to relief, including attorneys' fees and costs,  
23 restitution, declaratory relief, and a permanent injunction enjoining SPE from its  
24 unlawful and unfair practices. Plaintiffs also seek reasonable attorneys' fees and  
25 costs under applicable law including Federal Rule of Civil Procedure 23 and  
26 California Code of Civil Procedure § 1021.5.  
27  
28

1 **COUNT VI: Declaratory Judgment**

2 219. Plaintiffs reallege and incorporate by reference the allegations contained  
3 in each of the preceding paragraphs as if fully set forth herein.  
4

5 220. As previously alleged, Plaintiffs and the Nationwide Class have stated  
6 claims against SPE based on negligence and implied contract.  
7

8 221. SPE has failed to live up to its obligations to provide reasonable security  
9 measures for the PII of Plaintiffs and the Nationwide Class, as indicated by its  
10 corporate history of security breaches and the specific Data Breach that precipitated  
11 this lawsuit.  
12

13 222. In addition, the Data Breach has rendered SPE's system even more  
14 vulnerable to unauthorized access and requires that SPE immediately take even more  
15 stringent measures to currently safeguard the PII of Plaintiffs and the Nationwide  
16 Class going forward.  
17

18 223. An actual controversy has arisen in the wake of SPE's Data Breach  
19 regarding SPE's *current* obligations to provide reasonable data security measures to  
20 protect the PII of Plaintiffs and the Nationwide Class. On information and belief,  
21 SPE maintains that its security measures were, and remain, reasonably adequate. On  
22 information and belief, SPE further denies that it previously had or now has any  
23 obligation to better safeguard the PII of Plaintiffs and the Nationwide Class.  
24

25 224. Plaintiffs thus seek a declaration that to comply with its existing  
26 obligations, SPE must implement specific additional, prudent industry security  
27  
28

1 practices, as outlined below, to provide reasonable protection and security to the PII  
2 of Plaintiffs and the Nationwide Class.  
3

4 225. Specifically, Plaintiffs and the class seek a declaration that (a) SPE's  
5 existing security measures do not comply with its obligations, and (b) that to comply  
6 with its obligations, SPE must implement and maintain reasonable security measures  
7 on behalf of Plaintiffs and the Nationwide Class, including, but not limited to: (1)  
8 engaging third party security auditors/penetration testers as well as internal security  
9 personnel to conduct testing consistent with prudent industry practices, including  
10 simulated attacks, penetration tests, and audits on SPE's systems on a periodic basis;  
11 (2) engaging third party security auditors and internal personnel to run automated  
12 security monitoring consistent with prudent industry practices; (3) auditing, testing,  
13 and training its security personnel regarding any new or modified procedures; (4)  
14 purging, deleting and destroying, in a secure manner, employee data not necessary for  
15 its business operations; (5) conducting regular database scanning and securing checks  
16 consistent with prudent industry practices; (6) periodically conducting internal  
17 training and education to inform internal security personnel how to identify and  
18 contain a breach when it occurs and what to do in response to a breach consistent  
19 with prudent industry practices; (7) receiving periodic compliance audits by a third  
20 party regarding the security of the computer systems SPE uses to store the personal  
21 information of its current and former employees; (8) meaningfully educating its  
22 current and former employees about the threats they face as a result of the loss of  
23  
24  
25  
26  
27  
28

1 their PII to third parties, as well as the steps they must take to protect themselves; and  
2 (9) providing ongoing identity theft protection, monitoring, and recovery services to  
3 Plaintiffs and class members, as well as their dependents and designated beneficiaries  
4 of employment-related benefits through SPE.  
5

6 **COUNT VII: Violation of Virginia Code Annotated § 18.2-186.6**  
7

8 226. Plaintiffs reallege and incorporate by reference the allegations contained  
9 in each of the preceding paragraphs as if fully set forth herein.

10 227. Plaintiffs Corona and Springer bring this cause of action on behalf of the  
11 Virginia Class.  
12

13 228. SPE is an “entity” as defined by section 18.2-186.6(A).

14 229. Plaintiffs Corona and Springer and class members are “individuals” as  
15 defined by section 18.2-186.6(A).  
16

17 230. The PII of current and former SPE employees that was compromised and  
18 exposed in the Data Breach constitutes “personal information” as defined by section  
19 18.2-186.6(A), which includes Social Security numbers, driver’s license numbers,  
20 financial account numbers, and credit and debit card numbers in combination with  
21 security codes, access codes, or passwords that permit access to financial accounts.  
22

23 231. The breach of the PII of thousands of current and former SPE employees  
24 was a “breach of the security system” of SPE as defined by section 18.2-186.6(A).  
25

26 232. Under section 18.2-186.6(B), SPE was required to disclose any breach of  
27 the security of its system following discovery or notification of the breach to the  
28

1 Office of the Attorney General and any affected resident of the Commonwealth of  
2 Virginia without unreasonable delay.  
3

4 233. In violation of section 18.2-186.6(B), SPE unreasonably delayed  
5 informing Virginia Class members about the breach of their personal information,  
6 and failed to disclose to Virginia Class members without unreasonable delay that  
7 their unencrypted, or not properly and not securely encrypted, personal information  
8 had been breached.  
9

10 234. Upon information and belief, no law enforcement agency instructed SPE  
11 that notification to Virginia Class members would impede an investigation.  
12

13 235. As a result of SPE's violation of section 18.2-186.6, Virginia Class  
14 members have incurred and will incur economic damages to money or property,  
15 including but not necessarily limited to: (1) the diminution in the value of their PII  
16 entrusted to SPE for the purpose of deriving employment from SPE and with the  
17 understanding that SPE would safeguard their PII against theft and not allow access  
18 and misuse of their PII by others; (2) out-of-pocket costs associated with the  
19 prevention, detection, and recovery from identity theft and/or unauthorized use of  
20 financial and medical accounts; (3) lost opportunity costs associated with effort  
21 extended and the loss of productivity from addressing and attempting to mitigate the  
22 actual and future consequences of the breach, including but not limited to efforts  
23 spent researching how to prevent, detect, contest and recover from identity and health  
24 care/medical data misuse; (4) costs associated with the ability to use credit and assets  
25  
26  
27  
28

1 frozen or flagged due to credit misuse, including increased costs to use credit, credit  
2 scores, credit reports and assets; and (5) tax fraud and/or other unauthorized charges  
3 to financial, health care or medical accounts and associated lack of access to funds  
4 while proper information is confirmed and corrected.  
5

6 236. Plaintiffs further request that the Court order SPE to (1) identify and  
7 notify all members of the class who have not yet been informed of the Data Breach;  
8 and (2) notify affected current and former employees of any future data breaches by  
9 email within 24 hours of SPE's discovery of a breach or possible breach and by mail  
10 within 72 hours.  
11

12 237. Plaintiffs Corona and Springer, individually and on behalf of the  
13 Virginia Class, seek all remedies available under section 18.2-186.6, including but  
14 not limited to damages and equitable relief. Plaintiffs also seek reasonable attorneys'  
15 fees and costs under applicable law including Federal Rule of Civil Procedure 23 and  
16 California Code of Civil Procedure § 1021.5.  
17  
18

19 **Count VIII: Violation of Colorado Revised Statutes Annotated § 6-1-716**  
20

21 238. Plaintiffs reallege and incorporate by reference the allegations contained  
22 in each of the preceding paragraphs as if fully set forth herein.  
23

24 239. Plaintiff Forster brings this cause of action on behalf of the Colorado  
25 Class.  
26

27 240. SPE is a "commercial entity" as defined in section 6-1-716(1)(b).  
28



1           241. The PII of current and former SPE employees that was compromised and  
2 exposed in the Data Breach constitutes “personal information” as defined by section  
3 6-1-716(1)(d), which includes Social Security numbers, driver’s license numbers,  
4 account numbers or credit or debit card numbers, in combination with any required  
5 security code, access code, or password that would permit access to a resident’s  
6 financial account.  
7

9           242. The breach of the PII of thousands of current and former SPE employees  
10 was a “breach of the security of the system” of SPE as defined by section 6-1-  
11 716(1)(a).  
12

13           243. SPE violated section 6-1-716(2) through its unreasonable delay in  
14 informing Colorado Class members about the breach of their personal information,  
15 and failure to disclose to Colorado Class members without unreasonable delay that  
16 their unencrypted, or not properly and not securely encrypted, personal information  
17 had been breached.  
18

19           244. Upon information and belief, no law enforcement agency instructed SPE  
20 that notification to Colorado Class members would impede a criminal investigation.  
21

22           245. As a result of SPE’s violation of section 6-1-716, Colorado Class  
23 members have incurred and will incur economic damages, including but not  
24 necessarily limited to: (1) the diminution in the value of their PII entrusted to SPE for  
25 the purpose of deriving employment from SPE and with the understanding that SPE  
26 would safeguard their PII against theft and not allow access and misuse of their PII  
27  
28

1 by others; (2) out-of-pocket costs associated with the prevention, detection, and  
2 recovery from identity theft and/or unauthorized use of financial and medical  
3 accounts; (3) lost opportunity costs associated with effort extended and the loss of  
4 productivity from addressing and attempting to mitigate the actual and future  
5 consequences of the breach, including but not limited to efforts spent researching  
6 how to prevent, detect, contest and recover from identity and health care/medical data  
7 misuse; (4) costs associated with the ability to use credit and assets frozen or flagged  
8 due to credit misuse, including increased costs to use credit, credit scores, credit  
9 reports and assets; and (5) tax fraud and/or other unauthorized charges to financial,  
10 health care or medical accounts and associated lack of access to funds while proper  
11 information is confirmed and corrected.  
12  
13  
14  
15

16 246. Plaintiffs further request that the Court order SPE to (1) identify and  
17 notify all members of the Colorado Class who have not yet been informed of the Data  
18 Breach; and (2) notify affected current and former employees of any future data  
19 breaches by email within 24 hours of SPE's discovery of a breach or possible breach  
20 and by mail within 72 hours.  
21

22 247. Plaintiff Forster, individually and on behalf of the Colorado Class, seeks  
23 all remedies available under section 6-1-716, including but not limited to damages  
24 and equitable relief, and reasonable attorneys' fees and costs under applicable law.  
25  
26  
27  
28

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**IX. PRAYER FOR RELIEF**

Plaintiffs, on behalf of themselves and on behalf of the proposed classes,  
request that the Court:

- a. Certify this case as a class action, appoint Plaintiffs as class representatives, and appoint Plaintiffs’ counsel to represent the classes;
  - b. Find that SPE breached its duty to safeguard and protect the PII of Plaintiffs and the class members that was compromised in the Data Breach;
  - c. Award Plaintiffs and class members appropriate relief, including actual and statutory damages, restitution and disgorgement;
  - d. Award equitable, injunctive and declaratory relief as may be appropriate;
  - e. Award all costs, including experts’ fees and attorneys’ fees, and the costs of prosecuting this action;
  - f. Award pre-judgment and post-judgment interest as prescribed by law;
- and
- g. Grant additional legal or equitable relief as this Court may find just and proper.

**X. JURY TRIAL DEMANDED**

Plaintiffs hereby demand a trial by jury on all issues so triable.

1 Dated: March 2, 2015

Respectfully submitted,

2  
3 **KELLER ROHRBACK L.L.P.**

4 By: /s/ Lynn Lincoln Sarko

5 Lynn Lincoln Sarko, *Admitted pro hac vice*

6 lsarko@kellerrohrback.com

7 Gretchen Freeman Cappio, *Admitted pro hac vice*

8 gcappio@kellerrohrback.com

9 Cari Campen Laufenberg, *Admitted pro hac vice*

10 claufenberg@kellerrohrback.com

11 1201 Third Avenue, Suite 3200

12 Seattle, WA 98101

13 Telephone: (206) 623-1900

14 Facsimile: (206) 623-3384

15 Matthew J. Preusch

16 mpreusch@kellerrohrback.com

17 **KELLER ROHRBACK L.L.P.**

18 1129 State Street, Suite 8

19 Santa Barbara, CA 93101

20 Telephone: (805) 456-1496

21 Facsimile: (805) 456-1497

22 ***Proposed Interim Co-Lead Class Counsel and***  
23 ***Liaison Counsel***

24 Daniel C. Girard

25 dcg@girardgibbs.com

26 Amanda M. Steiner

27 as@girardgibbs.com

28 Linh G. Vuong

lgv@girardgibbs.com

**GIRARD GIBBS LLP**

601 California Street, 14th Floor

San Francisco, CA 94108

Telephone: (415) 981-4800

Facsimile: (415) 981-4846

Michael W. Sobol

msobol@lchb.com

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

RoseMarie Maliekel  
rmaliekel@lchb.com  
**LIEFF CABRASER HEIMANN &  
BERNSTEIN, LLP**  
275 Battery Street, 29th Floor  
San Francisco, CA 94111-3339  
Telephone: (415) 956-1000  
Facsimile: (415) 956-1008

Nicholas Diamand  
ndiamand@lchb.com  
**LIEFF CABRASER HEIMANN &  
BERNSTEIN, LLP**  
250 Hudson Street, 8th Floor  
New York, NY 10013-1413  
Telephone: (212) 355-9500  
Facsimile: (212) 355-9592

***Proposed Interim Co-Lead Class Counsel***

Hank Bates  
hbates@cbplaw.com  
Allen Carney  
acarney@cbplaw.com  
David Slade  
dslade@cbplaw.com  
**CARNEY BATES & PULLIAM, PLLC**  
11311 Arcade Drive  
Little Rock, AR 72212  
Telephone: (501) 312-8500  
Facsimile: (501) 312-8505

Raúl Pérez  
Raul.Perez@Capstonelawyers.com  
Jordan L. Lurie  
Jordan.Lurie@capstonelawyers.com  
Robert Friedl  
Robert.Friedl@capstonelawyers.com  
Tarek H. Zohdy  
Tarek.Zohdy@capstonelawyers.com  
Cody R. Padgett  
Cody.Padgett@capstonelawyers.com

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**CAPSTONE LAW APC**  
1840 Century Park East, Suite 450  
Los Angeles, CA 90067  
Telephone: (310) 556-4811  
Facsimile: (310) 943-0396

John H. Gomez  
john@gomeztrialattorneys.com  
John P. Fiske  
jfiske@gomeztrialattorneys.com  
Deborah Dixon  
ddixon@gomeztrialattorneys.com

**GOMEZ TRIAL ATTORNEYS**  
655 West Broadway, Suite 1700  
San Diego, CA 92101  
Telephone: (619) 237-3490  
Facsimile: (619) 237-3496

Joseph G.Sauder  
jgs@chimicles.com  
Matthew D. Schelkopf  
mds@chimicles.com  
Benjamin F. Johns  
bfj@chimicles.com  
Joseph B. Kenney  
jbk@chimicles.com  
**CHIMICLES & TIKELLIS LLP**  
One Haverford Centre  
361 West Lancaster Avenue  
Haverford, PA 19041  
Telephone: (610) 642-8500  
Facsimile: (610) 649-3633

Richard A. Maniskas, Esquire  
rmaniskas@rmclasslaw.com  
**RYAN & MANISKAS, LLP**  
995 Old Eagle School Road, Suite 311  
Wayne, PA 19087  
Telephone: (484) 588-5516  
Facsimile: (484) 450-2582

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Steven M. Tindall  
stindall@rhdtlaw.com  
Valerie Bender  
vbrender@rhdtlaw.com  
**RUKIN HYLAND DORIA & TINDALL LLP**  
100 Pine Street, Suite 2150  
San Francisco, CA 94111  
Telephone: (415) 421-1800  
Facsimile: (415) 421-1700

Katrina Carroll  
kcarroll@litedepalma.com  
Kyle A. Shamberg  
kshamberg@litedepalma.com  
**LITE DEPALMA GREENBERG, LLC**  
211 W. Wacker Drive, Suite 500  
Chicago, IL 60613  
Telephone: (312) 750-1265  
Facsimile: (312) 212-5919

*Additional Plaintiffs' Counsel*

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**CERTIFICATE OF SERVICE**

I, Lynn Lincoln Sarko, hereby certify that on March 2, 2015 I electronically filed **AMENDED CLASS ACTION COMPLAINT** with the Clerk of the United States District Court for the Central District of California using the CM/ECF system, which shall send electronic notification to all counsel of record.

/s/ Lynn Lincoln Sarko  
Lynn Lincoln Sarko