

1 Daniel C. Girard (State Bar No. 114826)
 2 dcg@girardgibbs.com
 3 Matthew B. George (State Bar No. 239322)
 4 mbg@girardgibbs.com
 5 **GIRARD GIBBS LLP**
 6 601 California Street, 14th Floor
 7 San Francisco, California 94104
 8 Telephone: (415) 981-4800
 9 Facsimile: (415) 981-4846

10 *Attorneys for Plaintiffs Joshua Forster and Ella Carline Archibeque*

11 **UNITED STATES DISTRICT COURT**
 12 **CENTRAL DISTRICT OF CALIFORNIA**

13 JOSHUA FORSTER and ELLA CARLINE
 14 ARCHIBEQUE, on behalf of themselves
 15 and all others similarly situated,

16 Plaintiffs,

17 vs.

18 SONY PICTURES ENTERTAINMENT
 19 INC.,

20 Defendant.

Case No. 2:14-cv-09646

CLASS ACTION

**COMPLAINT FOR RELIEF BASED
 ON:**

- (1) **Violation of the California Customer Records Act;**
- (2) **Violation of the Confidentiality of Medical Information Act;**
- (3) **Violation of the California Unfair Competition Law; and**
- (4) **Negligence**

DEMAND FOR JURY TRIAL

1 **SUMMARY OF THE CASE**

2 1. In late November 2014, thousands of current and former employees of Sony
3 Pictures Entertainment (“SPE”) learned that they were the victims of a massive data
4 breach that resulted in the posting of SPE’s personnel records on the internet. Among
5 other things, the data breach resulted in their names, home and email addresses, Social
6 Security numbers, visa and passport numbers, account routing information, salary and
7 retirement plan data, and health insurance and medical information being made public.
8 The employees’ records are posted on file-sharing websites for identity thieves to
9 download, have been published in news reports, and were used to send emails threatening
10 physical harm to employees and their families.

11 2. Cybercriminals were able to perpetrate a breach of this depth and scope
12 because SPE failed to maintain reasonable and adequate security measures to protect the
13 employees’ information from access and disclosure. SPE has statutory obligations to
14 protect its employees’ employment and personnel records from unauthorized access, yet
15 failed at numerous opportunities to prevent, detect, end, or limit the scope the breach.
16 Among other things, (1) SPE failed to implement security measures designed to prevent
17 this attack even though there have been similar cyber-attacks against SPE and its sister
18 companies, (2) SPE failed to employ security protocols to detect the hack and removal of
19 100 terabytes of data from its computer networks, and (3) SPE failed to maintain basic
20 security measures such as access controls, complex passwords and encryption so that if
21 data were accessed or stolen it would be unreadable.

22 3. Since the breach SPE has focused its remediation efforts on securing its
23 intellectual property from pirates and a public relations campaign directed at controlling
24 the damage associated with the release of embarrassing internal emails. Meanwhile, SPE
25 delayed confirming the data breach for a week and left its employees in the dark about
26 the scope of the breach, how they and their families were impacted, and what steps SPE
27 is taking to remedy or mitigate the breach. Due to SPE’s delay, employees have
28 purchased identify protection services and insurance yet still remain vulnerable to

1 identity theft, medical identity theft, tax fraud, and financial theft because their Social
2 Security numbers and medical information are still publicly available to anyone with an
3 internet connection. SPE's conduct is a direct cause of the harm employees are suffering
4 and will continue to experience for the indefinite future.

5 4. Plaintiffs are former SPE employees who bring this proposed class action
6 lawsuit on behalf of employees whose personal information has been compromised as a
7 result of the data breach. Plaintiffs allege that SPE failed to adequately safeguard its
8 current and former employees' personal information, including Social Security numbers,
9 medical records, and financial information, in compliance with applicable law. Plaintiffs
10 seek injunctive relief requiring SPE to implement and maintain security practices to
11 comply with regulations designed to prevent and remedy these types of breaches, as well
12 as restitution, damages, and other relief.

13 **PARTIES**

14 5. Plaintiff Joshua Forster is a resident of Denver, Colorado

15 6. Plaintiff Ella Carline Archibeque is a resident of Los Angeles, California.

16 7. Defendant Sony Pictures Entertainment Inc. ("SPE") is a multi-billion dollar
17 movie and television production and distribution company. SPE is incorporated in the
18 State of Delaware, with its principal place of business in Los Angeles, California.

19 **JURISDICTION AND VENUE**

20 8. This Court has original jurisdiction pursuant to the Class Action Fairness
21 Act, 28 U.S.C. § 1332(d), because (a) at least one member of the putative class is a
22 citizen of a state different from SPE, (b) the amount in controversy exceeds \$5,000,000,
23 exclusive of interest and costs, (c) the proposed class consists of more than 100 class
24 members, and (d) none of the exceptions under the subsection apply to this action.

25 9. This Court has jurisdiction over SPE because it is registered to conduct
26 business in California, it has sufficient minimum contacts in California, or otherwise
27 intentionally avails itself of the markets within California, through maintaining its
28 principal place of business in California and through the promotion, sale, marketing and

1 distribution of its products in California, to render the exercise of jurisdiction by this
2 Court proper and necessary.

3 10. Venue is proper in this District under 28 U.S.C. § 1391 because one of the
4 Plaintiffs resides in this district, SPE maintains its principal place of business in this
5 District, and a substantial part of the events giving rise to Plaintiffs' claims occurred in
6 this District.

7 **COMMON FACTUAL ALLEGATIONS**

8 **The Data Breach**

9 11. On November 24, 2014, the media reported that SPE was subject to an
10 undetected breach that extracted 100 terabytes of data from the company and caused the
11 leak of the personal, financial, and medical information of thousands of current and
12 former employees on the internet.

13 12. On November 30, 2014, hackers began releasing portions of stolen data to
14 the public, beginning with a series of unreleased movies produced by SPE. The media
15 then reported receiving emails with links to a file on Pastebin, a file-sharing site that
16 contained a trove of personnel information on SPE's employees. Information security
17 reporter Brian Krebs reported that the published files contained "sensitive data on tens of
18 thousands of Sony employees, including Social Security numbers, medical and salary
19 information." Mr. Krebs also observed files being traded on torrent networks, including a
20 global employee list containing names, employee IDs, usernames, and birthdates of
21 current and former SPE employees, and a list containing names, birthdates, Social
22 Security numbers, and health savings account data.¹ Other employee information
23 reportedly exposed in this data breach to date includes passport and visa information of
24 actors and production crews, email correspondence, and accounting data. Hackers also
25

26 _____
27 ¹ Brian Krebs, *Sony Breach May Have Exposed Employee Healthcare, Salary Data*,
28 Krebs on Security, <https://krebsonsecurity.com/2014/12/sony-breach-may-have-exposed-employee-healthcare-salary-data/> (last updated Dec. 2, 2014, 1:58 PM).

1 published a list of approximately 2,500 servers and 245 individual computers that the
2 hackers had access to at SPE offices in various locations to obtain the data.

3 13. Later, Social Security numbers for over 47,000 current and former SPE
4 employees were reportedly released. Some of these employees were last employed by
5 SPE as far back as 1955, raising concerns over the propriety of SPE's data retention
6 policies. Hackers have also used the stolen data to threaten SPE's employees and their
7 families with physical harm. On December 5, 2014, many former and current SPE
8 employees received an email in which they were told: "Please sign your name to object
9 the false [sic] of the company at the email address below if you don't want to suffer
10 damage. If you don't, not only you but your family will be in danger."²

11 14. The leaks are ongoing, with another batch of data released on December 8,
12 2014, containing detailed contact information for dozens of celebrities. Hackers have
13 threatened to release more data as Christmas approaches. Given the amount and
14 sensitivity of personal, financial, and medical information SPE maintains on its
15 employees, they are understandably "fearful of what additional information about them
16 and their colleagues could still appear online."³

17 **SPE Has Inadequate Security Practices Despite Prior Breaches**

18 15. The number of cyber-attacks aimed at major corporations has risen
19 dramatically in recent years. Even SPE's own sister companies, Sony Network
20 Entertainment International LLC and Sony Computer Entertainment America LLC,
21 experienced a massive data breach in 2011, which compromised the personal information
22 of approximately 77 million PlayStation Network users. In the same year, SPE itself

23 ² Dave McNary, *Hackers Threaten Sony Employees in New Email: 'Your Family Will Be*
24 *in Danger,* Variety (Dec. 5, 2014, 2:56 PM), [http://variety.com/2014/film/news/hackers-](http://variety.com/2014/film/news/hackers-threaten-sony-employees-in-new-email-your-family-will-be-in-danger-1201372230/)
25 [threaten-sony-employees-in-new-email-your-family-will-be-in-danger-1201372230/](http://variety.com/2014/film/news/hackers-threaten-sony-employees-in-new-email-your-family-will-be-in-danger-1201372230/).

26 ³ Rachel Emma Silverman & Ben Fritz, *Data Breach Sets Off Upheaval at Sony Pictures,*
27 *Wall St. J.,* [http://online.wsj.com/articles/data-breach-sets-off-upheaval-at-sony-pictures-](http://online.wsj.com/articles/data-breach-sets-off-upheaval-at-sony-pictures-1417657799)
28 [1417657799](http://online.wsj.com/articles/data-breach-sets-off-upheaval-at-sony-pictures-1417657799) (last updated Dec. 4, 2014, 10:14 AM).

1 experienced a data breach in which hackers stole personal data of over one million
2 customers.

3 16. Given the recent increase of data breaches aimed at major corporations and
4 SPE's own experiences, SPE must be more vigilant than ever of the need to adopt,
5 implement, and maintain security measures to protect its employees' personal
6 information. But SPE has publicly emphasized cost-savings over compliance when it
7 comes to data security. In 2007, SPE's executive director of information security was
8 interviewed by CIO Magazine regarding compliance with security and privacy
9 regulations. When discussing the risk analysis of protecting private data, Jason Spaltro
10 weighed the hypothetical cost of preventing a potential intrusion at \$10 million against
11 the hypothetical cost of responding to a breach at \$1 million. "With those numbers, says
12 Spaltro, 'it's a valid business decision to accept the risk' of a security breach. 'I will not
13 invest \$10 million to avoid a possible \$1 million loss,' he suggests."⁴

14 17. SPE's security practices continue to fall below industry standards. SPE
15 reportedly took a "remarkably lax approach to data security," reported Kevin Roose, a
16 well-regarded technological writer, given that some of the files released in this data
17 breach that contained personal employee data were "unencrypted Excel and Word files,
18 labeled plain as day."⁵ Time Magazine also reported a former employee's criticism of
19 SPE's information security team and that SPE largely ignored the employees' reports of
20 security violations. SPE dedicated insufficient resources to data security. The leaked
21 documents show that out of 7,000 employees, only *eleven* of those employees were
22

23 ⁴ Allan Holmes, *Your Guide to Good-Enough Compliance*, CIO (Apr. 6, 2007, 8:00 AM),
24 [http://www.cio.com/article/2439324/risk-management/your-guide-to-good-enough-
25 compliance.html](http://www.cio.com/article/2439324/risk-management/your-guide-to-good-enough-compliance.html).

26 ⁵ Kevin Roose, *More From The Sony Pictures Hack: Budgets, Layoffs, HR Scripts, and*
27 *3,800 Social Security Numbers*, Fusion, [http://fusion.net/story/30850/more-from-the-
28 sony-pictures-hack-budgets-layoffs-hr-scripts-and-3800-social-security-numbers/](http://fusion.net/story/30850/more-from-the-sony-pictures-hack-budgets-layoffs-hr-scripts-and-3800-social-security-numbers/) (last
visited Dec. 4, 2014).

1 assigned to the information security team, far too few for a multi-billion dollar company.⁶
2 SPE has also been previously criticized in security audits for the type of substandard
3 password and access control security practices that were ultimately exploited in the 2014
4 breach.

5 18. SPE has also failed to vigilantly employ intrusion prevention and detection
6 protocols that would have detected and prevented the breach. Some experts who have
7 analyzed the malicious software behind this data breach have suggested that the hackers
8 may have been inside SPE's network for some time, allowing them to become familiar
9 with the network. Other experts are criticizing SPE's use of private cryptographic keys,
10 which have been released with the leaked data. Access to cryptographic keys may have
11 allowed hackers to elude any systems intended to detect intrusions.⁷

12 19. Though SPE told its employees on December 8, 2014 that the attack is
13 "unprecedented in nature" and "undetectable by industry standard antivirus software,"
14 security researchers have expressed doubts regarding Sony's spin control. Adam Caudill,
15 an independent security researcher suggests, "To protect their image, [SPE] need[s] this
16 to be an unpreventable, incredibly sophisticated attack." Caudill added, "Even if they
17 couldn't detect the malware, they should have detected the unusual activity. You don't
18 steal such a large amount of data without raising some red flags – the question is, was
19 anyone watching?"⁸

21 ⁶ Sam Frizell, *Report: Sony's Security Team Was Unprepared for Hack*, TIME (Dec. 5,
22 2014), <http://time.com/3620288/sony-hack-unprepared/>.

23 ⁷ Joshua Brustein, *Experts: Sony Hackers Were Inside the Company Network for a Long*
24 *Time*, Bloomberg Businessweek (Dec. 3, 2014),
25 [http://www.businessweek.com/articles/2014-12-03/sony-hackers-were-inside-the-](http://www.businessweek.com/articles/2014-12-03/sony-hackers-were-inside-the-company-network-for-a-long-time)
26 [company-network-for-a-long-time](http://www.businessweek.com/articles/2014-12-03/sony-hackers-were-inside-the-company-network-for-a-long-time).

27 ⁸ Lorenzo Franceschi-Bicchierai, *Don't believe the hype: Sony hack not 'unprecedented,'*
28 *experts say*, Mashable (Dec. 8, 2014), [http://mashable.com/2014/12/08/sony-hack-](http://mashable.com/2014/12/08/sony-hack-unprecedented-undetectable/)
[unprecedented-undetectable/](http://mashable.com/2014/12/08/sony-hack-unprecedented-undetectable/).

1 **Current and Former SPE Employees Are Victims of the Breach**

2 20. In addition to implementing a sophisticated public relations campaign to
3 portray the breach as beyond its control, SPE focused its early remediation efforts on
4 controlling the damage associated with salacious comments appearing in emails about
5 movie stars and removing pirated films from the internet. Meanwhile, SPE has
6 repeatedly failed to provide its current and former employees with access to concrete
7 information about the breach, which of their data was published, and how SPE is
8 protecting their information moving forward. Calls and emails to SPE from affected
9 employees were routinely ignored or answered with rote and unhelpful responses.

10 21. It was not until the evening of December 2, 2014 that SPE finally issued an
11 official internal memo to 6,500 employees confirming that the data breach was authentic,
12 and “that a large amount of confidential Sony Pictures Entertainment data has been stolen
13 by the cyber attackers, including personnel information and business documents.” SPE
14 advised employees “to assume that information about [them] in the possession of the
15 company might be in [the hackers’] possession.”⁹ To date, SPE has yet to send a formal
16 notice of the breach to all former employees.

17 22. As a result of SPE’s negligent security practices and slow response to the
18 breach, former and current SPE employees are subject to an increased and concrete risk
19 of identity theft based on the SPE’s exposure of their personal and medical information
20 and have and will have to spend time and money securing their personal information,
21 accounts and protecting their identities. As SPE itself recommended, former and current
22 SPE employees will need to monitor their accounts and credit, and will also have to pay
23 for credit monitoring or credit reports in the wake of the data breach to make sure that
24 their credit and identity is not harmed by anyone who may have stolen their information.
25 Individuals whose bank information were compromised may have to pay fees to their

26 _____
27 ⁹ Ben Fritz, *Sony Executives Confirm Leaked Pay Data Is Authentic*, Wall St. J. (Dec. 3,
28 2014, 3:21 PM), <http://blogs.wsj.com/digits/2014/12/03/sony-executives-confirm-leaked-pay-data-is-authentic/>.

1 banks for new debit and credit cards, or have to pay fees to have the cards shipped faster
2 so that they do not have to wait weeks to make purchases on their accounts. These
3 individuals may also lose access to their funds and time and money by spending hours on
4 the phone or in person with banks and credit agencies trying to reverse unauthorized
5 charges, clear up credit issues, and order new cards.

6 23. Former and current SPE employees whose Social Security numbers have
7 been compromised have spent time contacting various agencies, such as the Internal
8 Revenue Service and the Social Security Administration. They also now face a real and
9 immediate risk of identity theft and other problems associated with the disclosure of their
10 Social Security number, and will need to monitor their credit and tax filings for an
11 indefinite duration. Individuals cannot even obtain a new Social Security number *until*
12 there is evidence of ongoing problems due to misuse of the Social Security number.
13 Even then, the Social Security Administration warns “that a new number probably will
14 not solve all [] problems . . . and will not guarantee [] a fresh start.” “For some victims of
15 identity theft, a new number actually creates new problems.”¹⁰

16 24. As a result of the November 2014 data breach, SPE employees’ medical
17 information has been posted to the internet where it has been viewed by members of the
18 media and the public, including complaints from employees about unpaid medical
19 insurance claims, spreadsheets that contained the health conditions and medical
20 procedures for employees with diagnoses such as cancer, heart disorders, and end-stage
21 renal disease, along with employees’ personally identifiable information that were
22 contained in the spreadsheets and other data released in the breach. SPE employees
23 whose medical and insurance information has been leaked will need to spend time to
24 monitor their medical bills, insurance records and credit reports. They may also be
25 fraudulently charged for unauthorized medical services or equipment, which will require
26

27 ¹⁰ *Identity Theft And Your Social Security Number*, Social Security Administration (Dec.
28 2013), <http://www.ssa.gov/pubs/EN-05-10064.pdf>.

1 them to spend time and money resolving these problems. They will also have to deal
2 with an increased risk of medical identity theft. Medical information is highly valuable
3 and is reportedly “worth 10 times more than [a person’s] credit card number on the black
4 market.”¹¹ According to the Office of Inspector General of the U.S. Department of
5 Health & Human Services, “[m]edical identity theft can disrupt [a person’s] life, damage
6 [] credit rating, and waste taxpayer dollars. The damage can be life-threatening [] if
7 wrong information ends up in [the victim’s] personal medical records.”¹²

8 **PLAINTIFFS’ EXPERIENCES**

9 **Plaintiff Joshua Forster**

10 25. Plaintiff Joshua Forster is a resident of Denver, Colorado. He resided in
11 California from 1999-2014. Plaintiff Forster was formerly employed by SPE within
12 Sony Pictures Imageworks as an associate systems administrator intern from January
13 2013 through April 2013. In April 2013, he began working as a contractor for SPE as an
14 associate systems administrator until February 2014. Prior to January 2013, Plaintiff
15 Forster worked on and off for various SPE subsidiaries and affiliates since 2006,
16 including Stage 6 Films and Screen Gems. During his employment, SPE obtained his
17 sensitive and personal information, including his Social Security number and contact
18 information.

19 26. Plaintiff Forster learned of the SPE data breach from watching the news on
20 television. The SPE data breach has compromised his personal data, including his Social
21 Security number, address, phone number, employment and salary information. Since
22 learning of the data breach, Plaintiff Forster has spent time contacting SPE to inquire

23 ¹¹ Caroline Humer & Jim Finkle, *Your medical record is worth more to hackers than your*
24 *credit card*, Reuters (Sept. 24, 2014, 2:24 PM),
25 [http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-](http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924)
26 [idUSKCN0HJ21I20140924](http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924).

27 ¹² *Medical ID Theft / Fraud Information*, U.S. Department of Health & Human Services,
28 <https://oig.hhs.gov/fraud/medical-id-theft/> (last visited Dec. 9, 2014).

1 about the data breach, cancelling his credit cards, contacting a credit bureau to set up
2 fraud alerts, and signing up for identity theft protection. Due to SPE's conduct, Plaintiff
3 Forster is now at a heightened risk for future identity theft.

4 **Plaintiff Ella Carline Archibeque**

5 27. Plaintiff Archibeque was formerly employed by SPE at various times from
6 approximately 2002-2009 as a Visual Effects Coordinator, Senior Marketing Manager,
7 and Coordinator, Asset Management within the Sony Pictures ImageWorks division.
8 During this time, and as a condition of employment, Plaintiff Archibeque shared sensitive
9 and personal information with SPE, including her Social Security number, date of birth,
10 contact information, and had other sensitive information in her personnel records such as
11 health and medical insurance and information that has been subject to the breach. She
12 expected that SPE would safeguard her personal information and employment records,
13 and that SPE would not retain information it no longer needed since she left employment
14 five years ago.

15 28. In late November 2014, Plaintiff Archibeque learned of the SPE data breach
16 on the internet and contacted SPE by email. She received a short response from SPE
17 informing her that someone would follow up with her.

18 29. Plaintiff Archibeque is cautious about protecting her identity as a result of
19 the breach, and is not aware of being a victim of identity theft in the past. Since learning
20 of the SPE data breach, she has enrolled in a credit monitoring service through LifeLock
21 and currently pays approximately \$20.00 a month. Due to SPE's conduct, Plaintiff
22 Archibeque is now at a heightened risk for future identity theft based on the theft and
23 disclosure of her personal information.

24 **CLASS ACTION ALLEGATIONS**

25 30. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure 23 on
26 behalf of themselves and the classes preliminarily defined as:

1 **Nationwide Class**

2 All former or current Sony Pictures employees in the United States whose
3 personal information was compromised as a result of the data breach
4 publicized in November 2014.

5 **California Class**

6 All former or current Sony Pictures employees that reside or have resided in
7 California and whose personal information was compromised as a result of
8 the data breach publicized in November 2014.

9 Excluded from the proposed classes are anyone employed by counsel for Plaintiffs in this
10 action; and any Judge to whom this case is assigned, as well as his or her staff and
11 immediate family.

12 31. Plaintiffs satisfy the numerosity, commonality, typicality, and adequacy
13 prerequisites for suing as a representative party pursuant to Rule 23.

14 32. Numerosity. The proposed classes consist of thousands of former or current
15 SPE employees who had their data stolen in the SPE data breach, making joinder of each
16 individual member impracticable.

17 33. Commonality. Common questions of law and fact exist for each of the
18 proposed class's claims and predominate over questions affecting only individual class
19 members.

20 For the Nationwide Class, common questions include:

21 a. Whether SPE had a legal duty to use reasonable security measures to protect
22 former or current employees' personal information;

23 b. Whether SPE breached its legal duty by failing to protect former or current
24 employees' personal information;

25 c. Whether SPE acted reasonably in securing its former or current employees'
26 personal information;

27 d. Whether any breach of SPE's legal duties caused Plaintiffs and the class
28 members to suffer damages; and

1 e. Whether Plaintiffs and class members are entitled to damages, restitution
2 and injunctive relief.

3 For the California Class, common questions include:

4 a. Whether SPE violated California Civil Code sections 1798.81.5 by failing to
5 implement reasonable security procedures and practices;

6 b. Whether SPE violated California Civil Code section 1798.82 by failing to
7 promptly notify class members that their personal information had been compromised;

8 c. Whether SPE violated California Civil Code section 56.20 by failing to
9 maintain the confidentiality of class members' medical information;

10 c. Whether class members may obtain damages, restitution, declaratory, and
11 injunctive relief against SPE under Civil Code sections 1798.84, 56.36(b)(1), or under the
12 UCL; and

13 d. What security procedures and data-breach notification procedure SPE should
14 be required to implement as part of any injunctive relief ordered by the Court.

15 34. Typicality. Plaintiffs' claims are typical of the claims of the proposed
16 classes because, among other things, Plaintiffs and class members sustained similar
17 injuries as a result of SPE's uniform wrongful conduct and their legal claims all arise
18 from the same core SPE practices.

19 35. Adequacy. Plaintiffs will fairly and adequately protect the interests of the
20 classes. Their interests do not conflict with class members' interests and they have
21 retained counsel experienced in complex class action and data privacy litigation to
22 vigorously prosecute this action on behalf of the classes.

23 36. In addition to satisfying the prerequisites of Rule 23(a), Plaintiffs satisfy the
24 requirements for maintaining a class action under Rule 23(b)(3). Common questions of
25 law and fact predominate over any questions affecting only individual members and a
26 class action is superior to individual litigation. The amount of damages available to
27 individual plaintiffs is insufficient to make litigation addressing SPE's conduct
28 economically feasible in the absence of the class action procedure. Individualized

1 litigation also presents a potential for inconsistent or contradictory judgments, and
2 increases the delay and expense to all parties and the court system presented by the legal
3 and factual issues of the case. By contrast, the class action device presents far fewer
4 management difficulties and provides the benefits of a single adjudication, economy of
5 scale, and comprehensive supervision by a single court.

6 37. In addition, class certification is appropriate under Rule 23(b)(1) or (b)(2)
7 because:

- 8 a. the prosecution of separate actions by the individual members of the
9 proposed classes would create a risk of inconsistent or varying
10 adjudication which would establish incompatible standards of conduct for
11 SPE;
- 12 b. the prosecution of separate actions by individual class members would
13 create a risk of adjudications with respect to them which would, as a
14 practical matter, be dispositive of the interests of other class members not
15 parties to the adjudications, or substantially impair or impede their ability
16 to protect their interests; and
- 17 c. SPE has acted or refused to act on grounds that apply generally to the
18 proposed classes, thereby making final injunctive relief or declaratory
19 relief described herein appropriate with respect to the proposed classes as
20 a whole.

21 **FIRST CAUSE OF ACTION**

22 **For Violation of the California Customer Records Act,**
23 **California Civil Code Section 1798.80, *et seq.***

24 38. Plaintiffs incorporate the above allegations by reference.

25 39. Plaintiffs bring this cause of action on behalf of the California Class whose
26 personal information is maintained by SPE and/or that was compromised in the
27 November 2014 data breach.

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

7 41. SPE is a “business” within the meaning of Civil Code section 1798.80(a).

8 42. Plaintiffs and members of the class are “individual[s]” within the meaning of
9 the Civil Code section 1798.80(d). Pursuant to Civil Code sections 1798.80(e) and
10 1798.81.5(d)(1)(C), “personal information” includes an individual’s name, Social
11 Security number, driver’s license or state identification card number, debit card and credit
12 card information, medical information, or health insurance information. “Personal
13 information” under Civil Code section 1798.80(e) also includes address, telephone
14 number, passport number, education, employment, employment history, or health
15 insurance information.

16 43. The breach of the personal data of thousands of former or current SPE
17 employees constituted a “breach of the security system” of SPE pursuant to Civil Code
18 section 1798.82(g).

19 44. By failing to implement reasonable measures to protect its former and
20 current employees’ personal data, SPE violated Civil Code section 1798.81.5.

21 45. In addition, by failing to promptly notify all affected former and current SPE
22 employees that their personal information had been acquired (or was reasonably believed
23 to have been acquired) by unauthorized persons in the data breach, SPE violated Civil
24 Code section 1798.82 of the same title. SPE’s failure to timely notify employees of the
25 breach has caused class members damages who have had to buy identity protection
26 services or take other measures to remediate the breach caused by SPE’s negligence.

27 46. By violating Civil Code sections 1798.81.5 and 1798.82, SPE “may be
28 enjoined” under Civil Code section 1798.84(e).

1 47. Accordingly, Plaintiffs request that the Court enter an injunction requiring
2 SPE to implement and maintain reasonable security procedures to protect customers' data
3 in compliance with the California Customer Records Act, including, but not limited to:
4 (1) ordering that SPE, consistent with industry standard practices, engage third party
5 security auditors/penetration testers as well as internal security personnel to conduct
6 testing, including simulated attacks, penetration tests, and audits on SPE's systems on a
7 periodic basis; (2) ordering that SPE engage third party security auditors and internal
8 personnel, consistent with industry standard practices, to run automated security
9 monitoring; (3) ordering that SPE audit, test, and train its security personnel regarding
10 any new or modified procedures; (4) ordering that SPE purge, delete, destroy in a
11 reasonable secure manner employee data not necessary for its business operations; (5)
12 ordering that SPE, consistent with industry standard practices, conduct regular database
13 scanning and securing checks; (6) ordering that SPE, consistent with industry standard
14 practices, periodically conduct internal training and education to inform internal security
15 personnel how to identify and contain a breach when it occurs and what to do in response
16 to a breach; and (7) ordering SPE to meaningfully educate its former and current
17 employees about the threats they face as a result of the loss of their personal information
18 to third parties, as well as the steps they must take to protect themselves.

19 48. Plaintiffs further request that the Court require SPE to (1) identify and notify
20 all members of the class who have not yet been informed of the data breach; and (2) to
21 notify affected former and current employees of any future data breaches by email within
22 24 hours of SPE's discovery of a breach or possible breach and by mail within 72 hours.

23 49. As a result of SPE's violation of Civil Code sections 1798.81.5, and
24 1798.82, Plaintiffs and members of the class have and will incur economic damages
25 relating to time and money spent remedying the breach, including but not limited to,
26 expenses for bank fees associated with the breach, any unauthorized charges made on
27 financial accounts, lack of access to funds while banks issue new cards, tax fraud, as well
28 as the costs of credit monitoring and purchasing credit reports.

1 57. SPE did not obtain class members' written authorization to disclose or
2 release their medical information, which must meet the following requirements pursuant
3 to section 56.21:

- 4 a. The authorization must be handwritten by the patient who signs it or
5 in typeface no smaller than 14-point font;
- 6 b. The authorization must be clearly separate from any other language on
7 the same page and must be executed by a signature that serves no
8 purpose other than to execute the authorization;
- 9 c. The authorization must be signed by the patient or the patient's legal
10 representative;
- 11 d. The authorization must specify the limitations on the types of medical
12 information to be disclosed;
- 13 e. the authorization must state the name or functions of the employer or
14 person disclosing the medical information, the persons or entities
15 authorized to receive the medical information, and the specific
16 limitations on the use of the medical information by the persons or
17 entities authorized to receive the medical information;
- 18 f. The authorization must specify the date after which the recipient is no
19 longer entitled to use the information; and
- 20 g. The authorization must advise the person signing the authorization of
21 the right to receive a copy of the authorization.

22 58. As a result of the November 2014 data breach, class members' medical
23 information has been posted to the internet where it has been viewed by members of the
24 media and the public, including complaints from employees about unpaid medical
25 insurance claims, spreadsheets that contained the health conditions and medical
26 procedures for employees for diagnoses such as cancer, heart disorders, and end-stage
27 renal disease, along with employees' personally identifiable information that was
28 contained in the spreadsheets and other data released in the breach. Among other things,

1 SPE is and was negligent in failing to maintain its former and current employees' medical
2 information in encrypted form; failing to use reasonable security procedures to prevent
3 unauthorized access to files containing the medical information; failing to use reasonable
4 authentication procedures so that the medical information could be tracked in case of a
5 security breach; by delaying in notifying its former and current employees that their
6 private medical information had been compromised; and by allowing undetected and
7 unauthorized access where employees' private medical files were kept, all in violation of
8 the CMIA and Health Insurance Portability and Accountability Act (HIPAA).

9 59. On behalf of themselves and the class, Plaintiffs seek an order requiring SPE
10 to cease its violations of the CMIA. Among other things, SPE should be required to stop
11 negligently handling its employees' medical information and institute reasonable security
12 procedures to protect their medical information in compliance with the CMIA, including
13 but not limited to: (1) ordering that SPE, consistent with industry standard practices,
14 engage third party security auditors/penetration testers as well as internal security
15 personnel to conduct testing, including simulated attacks, penetration tests, and audits on
16 SPE's systems on a periodic basis; (2) ordering that SPE engage third party security
17 auditors and internal personnel, consistent with industry standard practices, to run
18 automated security monitoring – particularly for employees' medical information; (3)
19 ordering that SPE audit, test, and train its security personnel regarding any new or
20 modified procedures designed to protect employees' medical information; (4) ordering
21 that SPE purge, delete, destroy in a reasonable secure manner employees' medical
22 information not necessary for its business operations; (5) ordering that SPE, consistent
23 with industry standard practices, conduct regular database scanning and securing checks;
24 (6) ordering that SPE, consistent with industry standard practices, periodically conduct
25 internal training and education to inform internal security personnel how to identify and
26 contain a breach when it occurs and what to do in response to a breach; and (7) ordering
27 SPE to meaningfully educate its former and current employees about the threats they face
28

1 as a result of the loss of their medical information to third parties, as well as the steps
2 they must take to protect themselves.

3 60. Plaintiffs further seek an award of up to \$1,000 in statutory damages for
4 each class member pursuant to section 56.36(b)(1) of the CMIA. An award of statutory
5 damages is necessary to deter future violations by SPE and other employers. Plaintiffs,
6 individually and on behalf of the members of the Nationwide Class, also seek reasonable
7 attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure
8 23 and California Code of Civil Procedure § 1021.5.

9 **THIRD CAUSE OF ACTION**

10 **For Unlawful and Unfair Business Practices Under**
11 **California Business and Professions Code § 17200, *et seq.***

12 61. Plaintiffs incorporate the above allegations by reference.

13 62. Plaintiffs bring this cause of action on behalf the Nationwide Class whose
14 personal and/or medical information was compromised as a result of the data breach
15 publicized in November 2014.

16 63. SPE's acts and practices, as alleged in this complaint, constitute unlawful
17 and unfair business practices, in violation of the Unfair Competition Law ("UCL"), Cal.
18 Bus. & Prof. Code § 17200, *et seq.*

19 64. SPE's acts and practices, as alleged in this complaint, constitute unlawful
20 and unfair practices in that they violate California Civil Code section 1798.80, *et seq.*, the
21 CMIA, HIPAA, and because SPE's conduct was negligent.

22 65. SPE's practices were unlawful and in violation of California Civil Code
23 section 1798.81.5(b) because SPE failed to take reasonable security measures in
24 protecting its former and current employees' personal data.

25 66. SPE's practices were also unlawful and in violation of California Civil Code
26 section 1798.82 because SPE unreasonably delayed informing Plaintiffs and members of
27 the class about the breach of security after SPE knew the data breach occurred.

28

1 67. SPE’s practices were unlawful and in violation of section 56.20 of the CMIA
2 because it did not establish proper procedures to secure the confidentiality of its former
3 and current employees’ medical information.

4 68. SPE’s practices were also unlawful and in violation of section 56.36(b) of
5 the CMIA by negligently releasing Plaintiffs’ and class members’ medical information
6 that was within SPE’s control.

7 69. SPE further violated HIPAA by failing to establish procedures to keep
8 employees’ medical information confidential and private.

9 70. The acts, omissions, and conduct of SPE constitute a violation of the
10 unlawful prong of the UCL because it failed to comport with a reasonable standard of
11 care and public policy as reflected in statutes such as the Information Practices Act of
12 1977, Cal. Civ. Code § 1798, *et seq.*, HIPPA, and the California Customer Records Act,
13 Cal. Civ. Code § 1798.80, *et seq.*, which seek to protect individuals’ data and ensure that
14 entities who solicit or are entrusted with personal data utilize reasonable security
15 measures.

16 71. In unduly delaying informing customers of the data breach, SPE engaged in
17 unfair business practices by engaging in conduct that undermines or violates the stated
18 policies underlying the California Customer Records Act and other privacy statutes. In
19 enacting the California Customer Records Act, the Legislature stated that: “[i]dentity
20 theft is costly to the marketplace and to consumers” and that “victims of identity theft
21 must act quickly to minimize the damage; therefore expeditious notification of possible
22 misuse of a person’s personal information is imperative.” 2002 Cal. Legis. Serv. Ch.
23 1054 (A.B. 700) (WEST). SPE’s conduct also undermines California public policy as
24 reflected in other statutes such as the Information Practices Act of 1977, Cal. Civ. Code §
25 1798, *et seq.*, which seeks to protect individuals’ data and ensure that entities who solicit
26 or are entrusted with personal data utilize reasonable security measures.

27 72. As a direct and proximate result of SPE’s unlawful business practices as
28 alleged herein, Plaintiffs and members of the class have suffered injury in fact. Plaintiffs

1 and the class have been injured in that their personal, financial, and medical information
2 has been compromised and are at risk for future identity theft and fraudulent activity on
3 their financial accounts. Class members have also lost money and property by
4 purchasing credit monitoring services they would not otherwise had to but for SPE's
5 unlawful and unfair conduct.

6 73. As a direct and proximate result of SPE's unlawful business practices as
7 alleged herein, Plaintiffs and class members face an increased risk of identity theft and
8 medical fraud, based on the theft and disclosure of their personal and medical
9 information.

10 74. As a result of SPE's violations, Plaintiffs and members of the class are
11 entitled to injunctive relief, including, but not limited to: (1) ordering that SPE,
12 consistent with industry standard practices, engage third party security
13 auditors/penetration testers as well as internal security personnel to conduct testing,
14 including simulated attacks, penetration tests, and audits on SPE's systems on a periodic
15 basis; (2) ordering that SPE engage third party security auditors and internal personnel,
16 consistent with industry standard practices, to run automated security monitoring; (3)
17 ordering that SPE audit, test, and train its security personnel regarding any new or
18 modified procedures; (4) ordering that SPE purge, delete, destroy in a reasonable secure
19 manner employee data not necessary for its business operations; (5) ordering that SPE,
20 consistent with industry standard practices, conduct regular database scanning and
21 securing checks; (6) ordering that SPE, consistent with industry standard practices,
22 periodically conduct internal training and education to inform internal security personnel
23 how to identify and contain a breach when it occurs and what to do in response to a
24 breach; and (7) ordering SPE to meaningfully educate its former and current employees
25 about the threats they face as a result of the loss of their personal information to third
26 parties, as well as the steps they must take to protect themselves.

27 75. Because of SPE's unfair and unlawful business practices, Plaintiffs and the
28 class are entitled to relief, including restitution to Plaintiffs and class members of their

1 costs incurred associated with the data breach and disgorgement of all profits accruing to
2 SPE because of its unlawful and unfair business practices, attorneys' fees and costs,
3 declaratory relief, and a permanent injunction enjoining SPE from its unlawful and unfair
4 practices.

5 76. Plaintiffs, individually and on behalf of the members of the Nationwide
6 Class, also seek reasonable attorneys' fees and costs under applicable law including
7 Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

8 **FOURTH CAUSE OF ACTION**

9 **Negligence**

10 77. Plaintiffs incorporate the above allegations by reference.

11 78. Plaintiffs bring this cause of action on behalf of the Nationwide Class whose
12 personal information was compromised as a result of the data breach publicized in
13 November 2014.

14 79. In collecting the personal, financial, and medical information of its
15 employees, SPE as the employer owed Plaintiffs and members of the class a duty to
16 exercise reasonable care in safeguarding and protecting that information. This duty
17 included, among other things, maintaining and testing SPE's security systems and taking
18 other reasonable security measures to protect and adequately secure the personal data of
19 Plaintiffs and the class from unauthorized access. SPE's security system and procedures
20 for handling the personal, financial, and medical information of its former and current
21 employees were intended to affect Plaintiffs and the class. SPE was aware that by taking
22 such sensitive information of its employees, it had a responsibility to take reasonable
23 security measures to protect the data from being stolen.

24 80. The duty SPE owed to Plaintiffs and members of the class to protect their
25 personal information is also underscored by the California Customer Records Act, CMIA
26 and HIPAA, which recognize the importance of maintaining the confidentiality of
27 personal and medical information and were established to protect individuals from
28 improper disclosure of their medical information.

1 81. Additionally, SPE had a duty to timely disclose to Plaintiffs and members of
2 the class that their personal information had been or was reasonably believed to have
3 been compromised. Timely disclosure was appropriate so that Plaintiffs and members of
4 the class could, among other things, report the theft of their Social Security numbers to
5 the Internal Revenue Service, monitor their credit reports for identity fraud, undertake
6 appropriate measures to avoid unauthorized charges on their debit card or credit card
7 accounts, and change or cancel their debit or credit card PINs (personal identification
8 numbers) to prevent or mitigate the risk of fraudulent cash withdrawals or unauthorized
9 transactions.

10 82. There is a very close connection between SPE's failure to take reasonable
11 security standards to protect its former and current employees' data and the injury to
12 Plaintiffs and the class. When individuals have their personal information stolen, they
13 are at risk for identity theft, and need to buy credit monitoring services and purchase
14 credit reports to protect themselves from identity theft.

15 83. SPE is morally to blame for not protecting the data of its former and current
16 employees by failing to take reasonable security measures. If SPE had taken reasonable
17 security measures, data thieves would not have been able to take the personal information
18 of thousands of former and current SPE employees.

19 84. The policy of preventing future harm weighs in favor of finding a special
20 relationship between SPE and the class. SPE's employees count on SPE as their
21 employer to keep their data safe and in fact are required to share sensitive personal and
22 medical data with employers as a condition of employment. If companies are not held
23 accountable for failing to take reasonable security measures to protect their employees'
24 personal information, they will not take the steps that are necessary to protect against
25 future data breaches. SPE's former executive security has previously disavowed the need
26 to invest in security compliance which has now caused Plaintiffs and class members harm
27 due to SPE's negligence.

28

1 85. It was foreseeable that if SPE did not take reasonable security measures, the
2 data of Plaintiffs and members of the class would be stolen. Major corporations like SPE
3 face a higher threat of security breaches than other smaller companies due in part to the
4 large amounts of data they possess, particularly since many SPE employees are high-
5 profile movie and television stars. SPE should have known to take precaution to secure
6 its employees' data, especially in light of the data breaches it experienced within the last
7 four years.

8 86. SPE breached its duty to exercise reasonable care in protecting the personal
9 information of Plaintiffs and the class by failing to implement and maintain adequate
10 security measures to safeguard its employees' personal information, failing to monitor its
11 systems to identify suspicious activity, and allowing unauthorized access to the personal
12 information of Plaintiffs and the class.

13 87. SPE breached its duty to timely notify Plaintiffs and the class about the data
14 breach. While SPE waited several days after discovering the data breach to inform its
15 current employees that their personal information had been or was reasonably believed to
16 have been compromised, it failed to altogether issue any notice to its former employees
17 affected by the breach.

18 88. But for SPE's failure to implement and maintain adequate security measures
19 to protect its employees' personal information and failure to monitor its systems to
20 identify suspicious activity, the personal information of Plaintiffs and members of the
21 class would not be stolen, and they would not be at a heightened risk of identity theft in
22 the future.

23 89. SPE's negligence was a substantial factor in causing harm to Plaintiffs and
24 members of the class.

25 90. As a direct and proximate result of SPE's failure to exercise reasonable care
26 and use commercially reasonable security measures, the personal information of SPE
27 employees was accessed by unauthorized individuals who could use the information to
28

1 commit identity fraud, medical fraud, or debit and credit card fraud. Plaintiffs and the
2 class face a heightened risk of identity theft in the future.

3 91. Plaintiffs and members of the class have also suffered economic damages,
4 including the purchase of credit monitoring services they would not have otherwise
5 purchased.

6 92. Neither Plaintiffs nor other members of the class contributed to the security
7 breach, nor did they contribute to SPE's employment of insufficient security measures to
8 safeguard employees' personal information.

9 93. Plaintiffs and the class seek compensatory damages and punitive damages
10 with interest, the costs of suit and attorneys' fees, and other and further relief as this
11 Court deems just and proper.

12 **PRAYER FOR RELIEF**

13 WHEREFORE, Plaintiffs, individually and on behalf of the proposed classes,
14 requests that the Court:

- 15 a. Certify this case as a class action on behalf of the classes defined above,
16 appoint Joshua Forster and Ella Carline Archibeque as class representatives,
17 and appoint Girard Gibbs as class counsel;
- 18 b. Award declaratory, injunctive and other equitable relief as is necessary to
19 protect the interests of Plaintiffs and other class members;
- 20 c. Award restitution and damages to Plaintiffs and class members in an amount
21 to be determined at trial;
- 22 d. Award Plaintiffs and class members their reasonable litigation expenses and
23 attorneys' fees;
- 24 e. Award Plaintiffs and class members pre- and post-judgment interest, to the
25 extent allowable; and
- 26 f. Award such other and further relief as equity and justice may require.
- 27
28

1 Dated: December 17, 2014

Respectfully Submitted,

2 **GIRARD GIBBS LLP**

3
4 By: /s/ Matthew B. George
5 Matthew B. George

6 Daniel C. Girard
7 Matthew B. George
8 601 California Street, 14th Floor
9 San Francisco, California 94108
10 Telephone: (415) 981-4800
11 Facsimile: (415) 981-4846

12 **DEMAND FOR JURY TRIAL**

13 Plaintiffs demand a trial by jury for all issues so triable.

14
15 Dated: December 17, 2014

Respectfully Submitted,

16 **GIRARD GIBBS LLP**

17
18 By: /s/ Matthew B. George
19 Matthew B. George

20 Daniel C. Girard
21 Matthew B. George
22 601 California Street, 14th Floor
23 San Francisco, California 94108
24 Telephone: (415) 981-4800
25 Facsimile: (415) 981-4846