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

Attorneys for Plaintiffs Joshua Forster and Ella Carline Archibeque

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

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

Plaintiffs,

vs.

SONY PICTURES ENTERTAINMENT INC.,

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

SUMMARY OF THE CASE

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

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

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

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

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

PARTIES

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

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

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

JURISDICTION AND VENUE

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

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

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

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

COMMON FACTUAL ALLEGATIONS

The Data Breach

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

12. On November 30, 2014, hackers began releasing portions of stolen data to the public, 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 personnel information on SPE's employees. Information security reporter Brian Krebs reported that the published files contained "sensitive data on tens of thousands of Sony employees, including Social Security numbers, medical and salary information." Mr. Krebs also observed files being traded on torrent networks, including a global employee list containing names, employee IDs, usernames, and birthdates of current and former SPE employees, and a list containing names, birthdates, Social Security numbers, and health savings account data.[1] Other employee information reportedly exposed in this data breach to date includes passport and visa information of actors and production crews, email correspondence, and accounting data. Hackers also

[1] Brian Krebs, *Sony Breach May Have Exposed Employee Healthcare, Salary Data*, 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).

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

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

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

SPE Has Inadequate Security Practices Despite Prior Breaches

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

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

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

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

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

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

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

[5] Kevin Roose, *More From The Sony Pictures Hack: Budgets, Layoffs, HR Scripts, and 3,800 Social Security Numbers*, Fusion, 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).

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

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

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

---

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

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

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

Current and Former SPE Employees Are Victims of the Breach

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

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

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

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

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

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

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

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

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

PLAINTIFFS' EXPERIENCES

Plaintiff Joshua Forster

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

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

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

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

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

Plaintiff Ella Carline Archibeque

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

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

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

CLASS ACTION ALLEGATIONS

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

Nationwide Class

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

California Class

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

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

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

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

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

For the Nationwide Class, common questions include:

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

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

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

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

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

For the California Class, common questions include:

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

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

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

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

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

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

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

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

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

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

a. the prosecution of separate actions by the individual members of the proposed classes would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for SPE;

b. the prosecution of separate actions by individual class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and

c. SPE has acted or refused to act on grounds that apply generally to the proposed classes, thereby making final injunctive relief or declaratory relief described herein appropriate with respect to the proposed classes as a whole.

FIRST CAUSE OF ACTION

For Violation of the California Customer Records Act,

California Civil Code Section 1798.80, *et seq.*

38. Plaintiffs incorporate the above allegations by reference.

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

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

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

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

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

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

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

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

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

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

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

50. Plaintiffs, individually and on behalf of the members of the California Class, seeks all remedies available under Civil Code section 1798.84, including, but not limited to: (a) damages suffered by members of the class; and (b) equitable relief.

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

SECOND CAUSE OF ACTION

For Violation of the Confidentiality of Medical Information Act Under California Civil Code § 56, *et seq.*

52. Plaintiffs incorporate the above allegations by reference.

53. Plaintiffs bring this cause of action on behalf of the Nationwide Class whose medical information is maintained by SPE and/or was released in the November 2014 data breach.

54. California's Confidentiality of Medical Information Act (CMIA), Cal. Civ. Code § 56, *et seq.*, requires employers like SPE to protect their employees' confidential medical information and not release private medical information without signed proper authorization.

55. SPE has violated section 56.20 of the CMIA, which requires an "employer who receives medical information [to] establish appropriate procedures to ensure the confidentiality and protection from unauthorized use and disclosure of that information." "These procedures may include, but are not limited to, instruction regarding confidentiality of employees and agents handling files containing medical information, and security systems restricting access to files containing medical information." SPE has violated section 56.20 of the CMIA by failing to maintain the confidentiality of class members' medical information and by failing to institute reasonable safeguards to protect their medical information from disclosure.

56. SPE also violated section 56.36(b) of the CMIA by negligently releasing class members' medical information.

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

a. The authorization must be handwritten by the patient who signs it or in typeface no smaller than 14-point font;

b. The authorization must be clearly separate from any other language on the same page and must be executed by a signature that serves no purpose other than to execute the authorization;

c. The authorization must be signed by the patient or the patient's legal representative;

d. The authorization must specify the limitations on the types of medical information to be disclosed;

e. the authorization must state the name or functions of the employer or person disclosing the medical information, the persons or entities authorized to receive the medical information, and the specific limitations on the use of the medical information by the persons or entities authorized to receive the medical information;

f. The authorization must specify the date after which the recipient is no longer entitled to use the information; and

g. The authorization must advise the person signing the authorization of the right to receive a copy of the authorization.

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

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

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

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

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

THIRD CAUSE OF ACTION

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

61. Plaintiffs incorporate the above allegations by reference.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

FOURTH CAUSE OF ACTION

Negligence

77. Plaintiffs incorporate the above allegations by reference.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

PRAYER FOR RELIEF

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

a. Certify this case as a class action on behalf of the classes defined above, appoint Joshua Forster and Ella Carline Archibeque as class representatives, and appoint Girard Gibbs as class counsel;

b. Award declaratory, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and other class members;

c. Award restitution and damages to Plaintiffs and class members in an amount to be determined at trial;

d. Award Plaintiffs and class members their reasonable litigation expenses and attorneys' fees;

e. Award Plaintiffs and class members pre- and post-judgment interest, to the extent allowable; and

f. Award such other and further relief as equity and justice may require.

Dated: December 17, 2014

Respectfully Submitted,

GIRARD GIBBS LLP

By: /s/ Matthew B. George
Matthew B. George

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

DEMAND FOR JURY TRIAL

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

Dated: December 17, 2014

Respectfully Submitted,

GIRARD GIBBS LLP

By: /s/ Matthew B. George
Matthew B. George

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