Michael W. Sobol (State Bar No. 194857)
msobol@lchb.com
RoseMarie Maliekel (State Bar No. 276036)
rmaliekel@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: 415.956.1000
Facsimile: 415.956.1008

Nicholas Diamand
Pro Hac Vice forthcoming
ndiamand@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
250 Hudson Street, 8th Floor
New York, NY 10013-1413
Telephone: 212.355.9500
Facsimile: 212.355.9592

Hank Bates (State Bar No. 167688)
hbates@cbplaw.com
Allen Carney
acarney@cbplaw.com
David Slade
dslade@cbplaw.com
CARNEY BATES & PULLIAM, PLLC
11311 Arcade Drive
Little Rock, AR 72212
Telephone: 501.312.8500
Facsimile: 501.312.8505

Attorneys for Plaintiffs Michael Levine and Felix Lionel and the Proposed Class

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA
WESTERN DIVISION

MICHAEL LEVINE and FELIX LIONEL, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

SONY PICTURES ENTERTAINMENT, INC.

Defendant.

CASE NO. 2:14-cv-9687

COMPLAINT

CLASS ACTION

JURY TRIAL DEMANDED

I. INTRODUCTION

1. Beginning on November 21, 2014, and continuing to the present day, Defendant Sony Pictures Entertainment, Inc. ("Defendant") has been experiencing a massive data breach where the personally identifiable information ("PII") maintained by Defendant of its over 47,000 current and former employees and their families has been obtained and posted on websites across the Internet by a group calling itself the "Guardians of Peace" ("#GOP").

2. The publicly disclosed PII from the data maintained by Defendant contains the most intimate details of personal and professional lives including, but not limited to, medical records, Social Security Numbers, birth dates, personal emails, home addresses, salaries, tax information, employee evaluations, disciplinary actions, criminal background checks, severance packages, and family medical histories.

3. Defendant has failed to take reasonable steps to secure the data of its employees from hacking and other collateral attacks despite its having a duty to safeguard its employees' data. Only three years ago, Defendant incurred one of the largest data breaches in history, in which 77 million customer records were compromised. In the wake of that data breach, Defendant conceded that a "known vulnerability" was exploited, and subsequent analysis from the information technology community confirmed that Defendant had failed to put into place even the most rudimentary security protocols.

4. As a result of the staggering array of PII that has been compromised, Plaintiffs and Class Members, as well as their family members, will have to remain vigilant for the rest of their lives to combat potential identity theft arising from the critical, irreplaceable data such as Social Security Numbers, birth dates, and medical records that are not only in the hands of cyber criminals, but that also have been posted on the Internet for *anyone* to gather and use for any purpose, at any point, in perpetuity. Further, beyond the risk of identity theft, much of the PII is of

such a sensitive nature that unauthorized review by any third party for any purpose would amount to a grave invasion of privacy. Despite all best efforts of Plaintiffs, Class Members, or any other third party to scrub these data from the World Wide Web, they are forever recoverable by anyone who wishes to find them.

5. Defendant engages in the entertainment industry as part of a vast multinational corporate conglomerate, knows or should know that it may be the target of the world's most sophisticated data hackers or cybercriminals, and therefore Defendant has a duty subject to a standard of care that will protect its employees' PII from the possibility of such sophisticated hacking. This standard of care applies to Defendant regardless of the identity of the hackers or cybercriminals, even if, as some recent press reports indicate, they act at the direction of a foreign government. Defendant should have reasonably anticipated the possibility of such a cyber attack from the world's most sophisticated hackers, but failed to take adequate steps to protect against that possibility.

6. Defendant, as the employer of Plaintiffs and Class Members, owed them a duty of care in the acquisition and retention of their PII. Defendant breached this duty by failing to properly invest in adequate IT security. Defendant's acts and omissions complained of herein amply support Plaintiffs' claims of negligence; violations of California's data breach notification law, Cal. Civ. Code § 1798.80, *et seq.*; violations of California's medical records retention law, Cal. Civ. Code § 56, *et seq.*; bailment; and invasions of privacy under California common law as well as an invasion of the right to privacy guaranteed by the California Constitution.

II. THE PARTIES

7. Between 2003 and 2012, Plaintiff Michael Levine was a Technical Director for Sony Pictures Imageworks ("Imageworks"), a subsidiary of Defendant Sony Pictures Entertainment. As a result of Plaintiff Levine's employment, Defendant maintains and has access to his personal information, and information

concerning his wife, which he reasonably expects will be guarded and kept confidential. This information includes, but is not limited to, his social security number, his home address, his bank account information, his health care information, his employment history, his salary history, paystubs, and exit interview memoranda.

8. Plaintiff Lionel Felix is an IT professional based in Austin, Texas. Between 2001 and 2004, Mr. Felix was a Director of Technology for Defendant, during which time he ran IT infrastructure for Sony Pictures Digital Entertainment. As a result of Plaintiff Felix's employment, Defendant had access to his personal information which he reasonably expected would be guarded and kept confidential. This information included, but is not limited to, his social security number, his home address, his bank account information, his health care information, his employment history, his salary history, paystubs, and exit interview memoranda.

9. Defendant Sony Pictures Entertainment, Inc. is a Delaware corporation headquartered in Culver City, California and is an American entertainment subsidiary of Sony Corporation, a Japanese multinational corporation.

III. JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this putative nationwide class action pursuant to 28 U.S.C. § 1332 because the matter in controversy exceeds $5,000,000.00, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of states different than Defendant. *See* 28 U.S.C. § 1332(d)(2)(A).

11. This Court has personal jurisdiction over Defendant because it is headquartered in California, and because it conducts substantial business throughout California.

12. Venue is proper in this District under 28 U.S.C. § 1391 because a substantial part of the events giving rise to Plaintiffs' claims occurred within this District.

IV. FACTUAL ALLEGATIONS

A. A Breach of Data Maintained by Defendant's Exposed Confidential Information of Plaintiffs and Numerous Other Current and Former Employees of Defendant.

13. On November 21, 2014, Defendant's senior executives, including Chief Executive Officer Michael Lynton, received an anonymous email demanding "monetary compensation…or Sony Pictures will be bombarded as a whole." On information and belief, over the next three days, a message began to appear on Defendant's employees' computers, bearing a heading, "Hacked By #GOP." The content of the message stated "[w]e've obtained all your internal data…if you don't obey us, we'll release data…to the world."

14. Upon information and belief, "#GOP" is an as-of-yet-unidentified group of persons who refer to themselves as "Guardians of Peace." As used herein, "#GOP" refers to any and all persons or entities who have breached and obtained data files of Defendant which contain PII of its current and former employees and their families.

15. Over the past two weeks, #GOP has posted digital files and other information which were maintained by Defendant, thereby exposing its employees' sensitive PII including employment and medical records, human resources ("HR") documents, criminal background checks, hiring information, termination decisions, severance packages, disciplinary write-ups, payroll and bonus information, Social Security Numbers ("SSNs") coupled with additional personal information, and passport and visa scans.

16. The volume of exposed PII from Defendant demonstrates that both Defendant's approximately 6,500 current employees as well as tens of thousands of former employees and contractors, including individuals with records dating as far

back as the 1980s, have had their PII publicly exposed. Further, the exposed PII also contains the PII of current and former employees' family members.

17. The security firm Identity Finder LLC scanned 33,000 of the leaked documents and found more than 47,000 unique, exposed SSNs, appearing more than 1.1 million times inside 601 files. Most of the files containing SSNs also included additional PII, such as full names, dates of birth, and home addresses. PII containing SSNs are typically the principal data utilized by identity thieves. The public exposure of the PII maintained by Defendant presents a lifelong increased risk of identity theft to its current and former employees and their families.

18. The public exposure of PII maintained by Defendant includes sensitive health records of employees and their families. Upon information and belief, among the information publicly disclosed are Defendant's HR memos discussing the medical records of employees with particularly costly treatment requirements, including premature births, cancer, kidney failure, and liver cirrhosis. Other disclosed information includes detailed discussions with insurers over denied claims for surgeries and speech therapy sessions.

19. On December 5, 2014, certain of Defendant's employees received an email purportedly from the #GOP demanding that the recipient "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 the recipient failed to comply, the email continued, "not only you but your family will be in danger."

20. #GOP purports to have obtained from the PII maintained by Defendant "tens of terabytes" of data, though it states that, to date, it has only released one terabyte. On December 14, 2014, #GOP issued a statement promising a "Christmas present," claiming that "[t]he gift will be larger quantities of data. And it will be more interesting. The gift will surely give you much more pleasure and put Sony Pictures into the worst state."

21. For decades, Defendant failed, and continues to fail, to take the reasonably necessary actions to provide a sufficient level of IT security to reasonably secure its employees' PII. As a result of failing to devote adequate resources to its IT security, disregarding advice from third-party security auditors, and failing to take reasonable remedial measures after *prior breaches of data maintained by Defendant*, the PII maintained by Defendant was obtained by #GOP (herein, the "Sony Data Breach").

B. "Security at Sony Pictures wasn't just breached, it was abandoned."

22. None of the PII obtained by #GOP from the data maintained by Defendant—including spreadsheets of SSNs, medical records, disciplinary records, and criminal background checks, among others—had sufficient encryption or password protection. Rather, the PII obtained by #GOP from Defendant included unencrypted lists of account passwords and logins. For example, one file called "computer passwords" reportedly contained user credentials for logging onto the corporate network, while another entitled "Social Password Log" contained passwords for movie accounts on social media, which is likely the means used by hackers to compromise many of Defendant's movie accounts. A particularly damaging news story described a captured folder, containing thousands of logins and passwords in clear-text files, without password protection and actually labeled "PASSWORD." The PII obtained by #GOP also included digital certificates ordinarily used to secure computers and data.

23. Defendant's failure to safeguard its employees' PII was in part a function of its deliberate policy to avoid costs of providing adequate data security in the face of inevitable risk of a data breach. For example, in 2007, Sony's Executive Director of Information Security, Jason Spaltro, said in an interview that he was unwilling to invest the resources necessary to defend the company's sensitive information:

> It's a valid business decision to accept the risk. I will not invest $10 million to avoid a possible $1 million loss.

24. Defendant's failure to invest in adequate security left it vulnerable to serial data security breaches.

25. Earlier in 2014, Defendant's operations in Brazil fell prey to hackers. Although PII of 759 individuals was compromised, Defendant again deliberately failed to take remedial action. Jason Spaltro, on behalf of Sony, again commented that:

> … at this point, it appears that business contact information (name, address, email address) for 759 individuals associated with theaters in Brazil was exfiltrated from SpiritWorld. The information was contained in .txt versions of invoices for the theaters. In terms of a notification obligation, Brazil does not have a breach notification law. Although the Brazilian Constitution, Civil Code, and Consumer Protection Code contain general provisions on privacy protection, and data subjects are entitled to indemnification for moral and material damages that result from a violation of their privacy, **based on the facts known thus far I recommend against providing any notification to individuals given (a) the lack of a notification requirement; (b) the limited data fields involved; and (c) the fact that notifying would not likely have much effect in terms of mitigating potential damages**.

(Emphasis added).

26. In 2011, for a period of three months, Defendant suffered a series of global hacks to its PlayStation Network ("PlayStation Breach"), resulting in one of the largest data breaches in history, with the loss of unencrypted information from 77 million customer accounts, 12 million of which contained credit card numbers. The Company was called upon by the United States Congress (as well as regulatory bodies throughout the world) to answer questions with regard to the breach, and was the subject of multiple class action lawsuits in the US and Canada.

27. Much like the events giving rise to the current Sony Data Breach, the PlayStation Breach was foreshadowed by a warning from cyber criminals, stating:

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

28. Following the PlayStation Breach, numerous facts came to light detailing myriad security failings. Among them, Sony Corporation Chief Information Officer Shinji Hasejima admitted that Sony's Network was not secure at the time of the PlayStation Breach, stating the attackers exploited a "known vulnerability." Further, it came to light that Defendant invested significant resources, including firewalls, debug programs, and IP address limitations, to protect its *own* confidential proprietary information housed on Defendant's "development server," *without* incorporating the same safeguards on the PlayStation network (such as a basic firewall). Defendant's decision not to install and maintain appropriate firewalls on its network deviated from widespread industry practice and standards. Indeed, at the time, numerous experts in the field attributed the PlayStation Breach to an unsophisticated method of hacking that would not have been successful if Defendant had even the most basic security measures in place.

29. A recent Bloomberg article states that, although Defendant significantly improved the security of the PlayStation network, it failed to address glaring security vulnerabilities across its other networks, including those that pertain to the PII obtained by #GOP:

> Unlike banks and government agencies that are accustomed to deflecting high-level hacking attacks, Sony has been poorly prepared for the intrusions in part because its decentralized structure means security improvements in one division don't necessarily translate to other units, the people familiar with the investigations and other security experts said.

30. Defendant conducted multiple security audits, both internal and external, which would reasonably put it on notice of its security vulnerabilities and

the likely consequences of failing to address those vulnerabilities. For instance, a PriceWaterhouseCoopers audit dated September 25, 2014 found that Defendant's information technology security team failed to monitor firewalls within its operational oversight, as well as more than 100 other devices under its responsibility. That audit also reported that, since transitioning from a third-party vendor in September 2013, Defendant had failed to notify and direct the security team to monitor newly added devices, such as web servers and routers.

31. As of the time #GOP breached the PII maintained by Defendant, Defendant knew or should have known that it was failing to adequately safeguard the PII of its employees and their families, and that the PII was vulnerable to attack and acquisition by outside parties.

CLASS ALLEGATIONS

32. Plaintiffs bring this nationwide class action, pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following Class:

> All current and former employees of Defendant, and such employees' families, within the United States whose personally identifiable information maintained by Defendant was obtained by any third party in the Sony Data Breach.

33. Excluded from the Class are the following individuals and/or entities: Defendant and its parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments including, but not limited to, their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

34. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

35. The Class is so numerous that joinder of all members is impracticable. Upon information and belief, there are at least tens of thousands of individuals whose PII has been compromised as a result of the Sony Data Breach. The number of separate individuals is identifiable and ascertainable based on Defendant's records.

36. There are questions of law or fact common to the Class. These questions include, but are not limited to, the following:

a. Whether Defendant violated Cal. Civ. Code § 1798.80, *et seq.*;

b. Whether Defendant violated Cal. Civ. Code § 56 *et seq.*;

c. Whether Defendant's acts and omissions described herein give rise to a claim of negligence;

d. Whether Defendant's acts and omissions described herein give rise to a claim of bailment;

e. Whether Defendant's acts and omissions described herein give rise to a claim of invasion of privacy; and

f. Whether Defendant's acts and omissions described herein violated Plaintiffs' and Class Members' right to privacy, as guaranteed by the California Constitution.

37. Plaintiffs' claims are typical of the claims of the Class in that Plaintiffs and the Class had their PII compromised as a result of the Sony Data Breach, the cause of which was Defendant's acts and omissions, as complained of herein. Plaintiffs and Class Members are entitled to declaratory relief, statutory damages, restitution, and injunctive relief as a result of the conduct complained of herein. Moreover, upon information and belief, the conduct complained of herein is systemic. Thus, the representative Plaintiffs, like all other Class Members, face substantial risk of the same injury in the future. The factual basis of Defendant's

conduct is common to all Class Members, and represents a common thread of conduct resulting in injury to all members of the Class. Plaintiffs have suffered the harm alleged and have no interests antagonistic to any other Class Member.

38. Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs' interests do not conflict with the interests of the Class Members. Furthermore, Plaintiffs have retained competent counsel experienced in class action litigation. Plaintiffs' counsel will fairly and adequately protect and represent the interests of the Class. Fed. R. Civ. P. 23(a)(4) and 23(g) are satisfied.

39. Plaintiffs assert that pursuant to Fed. R. Civ. P. 23(b)(3), questions of law or fact common to the Class Members predominate over any questions affecting only individual members.

40. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Arguably, no Class Member could afford to seek legal redress individually for the claims alleged herein. Therefore, absent a class action, the Class Members will continue to suffer losses and Defendant's misconduct will proceed without remedy.

41. Even if Class Members themselves could afford such individual litigation, the court system could not. Given the complex legal and factual issues involved, and considering that the Class could number in the tens of thousands or greater, individualized litigation would significantly increase the delay and expense to all parties and to the Court. Individualized litigation would also create the potential for inconsistent or contradictory rulings. By contrast, a class action presents far fewer management difficulties, allows claims to be heard which may otherwise go unheard because of the relative expense of bringing individual lawsuits, and provides the benefits of adjudication, economies of scale and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT ONE
Negligence

42. Plaintiffs adopt and incorporate each and every allegation of this Complaint as if stated fully herein.

43. Defendant owed a duty to Plaintiffs and members of the Class to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their personal information in its possession from being compromised, lost, stolen, accessed and misused by unauthorized persons. This duty included, among other things, designing, implementing, maintaining and testing Defendant's security systems and protocols, consistent with industry standards and requirements, to ensure that Plaintiffs' and Class Members' PII in Defendant's possession was adequately secured and protected. Defendant further owed a duty to Plaintiffs and Class Members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

44. Defendant owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate security practices. Defendant solicited, gathered, and stored the personal data provided by Plaintiffs and members of the Class in the regular course of its business. Defendant knew it inadequately safeguarded such information on its computer systems, that its networks had suffered multiple data breaches in the past, and that both internal and third party auditors had identified systemic structural weaknesses in Defendant's IT security. Defendant knew that a breach of its systems would cause damages to Plaintiffs and members of the Class, and Defendant had a duty to adequately protect such sensitive PII.

45. Similarly, Defendant owed a duty to Plaintiffs and Class Members to timely disclose any incidents of data breaches, where such breaches compromised

the PII of Plaintiffs and Class Members. Plaintiffs and Class Members were foreseeable and probable victims of any inadequate notice practices. Defendant knew that, through its actions and omissions, it had caused the PII of Plaintiffs and Class Members to be compromised by malicious third parties, and that those third parties manifested an intent to do harm to Plaintiffs and Class Members. Such harm could only be mitigated by Plaintiffs and Class Members with timely notice of the Sony Data Breach.

46. Defendant breached its duties owed to Plaintiffs and Class Members (1) by failing to exercise reasonable care in the adoption, implementation, and maintenance of adequate IT security procedures, infrastructure, personnel, and protocols and (2) by failing to timely notify Plaintiffs and Class Members of the Sony Data Breach.

47. Defendant's breach of its duties owed to Plaintiffs and members of the Class caused injuries to Plaintiffs and members of the Class including, but not limited to, (a) theft of their PII; (b) costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts and medical records; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Sony Data Breach including, without limitation, finding fraudulent charges, cancelling and reissuing credit cards and bank accounts, purchasing credit monitoring and identity theft protection, and the stress, nuisance and annoyance of dealing with all issues resulting from the Sony Data Breach in the weeks leading up to and beyond the end-of-year holiday season; (d) the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and being posted for public consumption on the Internet; (e) damages to and diminution in value of their PII entrusted to Defendant for the purpose of deriving employment from Defendant and with the understanding that Defendant would safeguard their data against theft

and not allow access and misuse of their data by others; and (f) the continued risk to their PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect data in its possession.

48. But for Defendant's negligent and wrongful breach of its duties owed to Plaintiffs and the Class, Plaintiffs and the Class would not have been harmed and could have taken remedial measures to protect their PII.

49. Plaintiffs and Class Members seek an award of actual damages.

COUNT TWO
(Violation of Cal. Civ. Code § 1798.80, *et seq*.)

50. Plaintiffs adopt and incorporate each and every allegation of this Complaint as if stated fully herein.

51. The Sony Data Breach described herein was a "breach of the security system" within the meaning of Cal. Civ. Code § 1798.82(g).

52. The information lost in the Sony Data Breach was "personal information" as defined in Cal. Civ. Code § 1798.80(e).

53. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the PII being acquired, processed, and stored in the ordinary course of Defendant's business, as required by Cal. Civ. Code § 1798.81.5.

54. Further, upon failing to take the appropriate security measures, and upon discovering the Sony Data Breach, Defendant failed to notify Plaintiffs and Class Members of the Sony Data Breach, as required by Cal. Civ. Code § 1798.80, *et seq*.

55. As a result of Defendant's violations of Cal. Civ. Code § 1798.80 *et seq*., Plaintiffs and Class Members have sustained damages, including (a) theft of their PII; (b) costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts and medical records; (c) costs

associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Sony Data Breach including, without limitation, finding fraudulent charges, cancelling and reissuing credit cards and bank accounts, purchasing credit monitoring and identity theft protection, and the stress, nuisance and annoyance of dealing with all issues resulting from the Sony Data Breach in the weeks leading up to and beyond the end-of-year holiday season; (d) the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and being posted for public consumption on the Internet; (e) damages to and diminution in value of their PII entrusted to Defendant for the purpose of deriving employment from Defendant and with the understanding that Defendant would safeguard their data against theft and not allow access and misuse of their data by others; and (f) the continued risk to their PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect data in its possession.

56. Plaintiffs, individually and on behalf of the Class, seek all remedies available under Cal. Civ. Code § 1798.80, *et seq*., including actual and statutory damages, equitable relief, and reasonable attorney's fees.

COUNT THREE
Violations of Cal. Civ. Code § 56, *et seq*.

57. Plaintiffs adopt and incorporate each and every allegation of this Complaint as if stated fully herein.

58. Pursuant to Cal. Civ. Code § 56.20(a)

> Each employer who receives medical information shall 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.

59. Much of the PII held by Defendant, as an employer of Plaintiffs and Class Members, was the "medical information" of Plaintiffs and Class Members, as defined by Cal. Civ. Code § 56.05(j).

60. Accordingly, at all times relevant to this litigation, Defendant had a duty to provide adequate security for the medical information of Plaintiffs and Class Members.

61. Defendant breached this duty by failing to implement and maintain adequate IT security procedures, which failures in turn resulted in the Sony Data Breach.

62. As a result of the Sony Data Breach, Plaintiffs' and Class Members' medical information was obtained by third parties including, but not limited to, #GOP, without the authorization of Plaintiffs or Class Members.

63. Pursuant to Cal. Civ. Code § 56.36, Plaintiffs and Class Members are entitled to statutory damages of $1,000, as well as actual damages sustained as a result of the disclosure of their medical information through the Sony Data Breach.

COUNT FOUR
Bailment

64. Plaintiffs adopt and incorporate each and every allegation of this Complaint as if stated fully herein.

65. Plaintiffs and Class Members delivered and entrusted their PII to Defendant for the purpose of enabling Defendant to conduct its administrative business with its employees (Plaintiffs and Class Members).

66. A bailment arises where possession, but not ownership, of property is transferred from one party ("bailor") to another ("bailee"). Where a bailee has received a bailment from a bailor, a duty of care is owed. Typically, a bailee is strictly liable for the bailment.

67. During the period of bailment, Defendant, as bailee, owed Plaintiffs and Class Members a duty of care to safeguard their PII by maintaining reasonable security procedures and practices to protect such information. As alleged herein, Defendant breached this duty.

68. As a result of Defendant's breach of this duty, Plaintiffs and all other Class Members have been harmed as alleged herein.

COUNT FIVE
(Invasion of Privacy – Intrusion, Public Disclosure of Private Facts, Misappropriation of Likeness and Identity, and California Constitutional Right to Privacy)

69. Plaintiffs adopt and incorporate each and every allegation of this Complaint as if stated fully herein.

70. Plaintiffs and Class Members had a reasonable expectation of privacy in the PII unlawfully obtained in the Sony Data Breach including, but not limited to, information related to medical and health care records, human resources, employment and personnel file.

71. By failing to keep Plaintiffs' and Class Members' PII safe, by misusing Plaintiffs' and Class Members' PII, and by disclosing Plaintiffs' and Class Members' PII to unauthorized parties for unauthorized use, Defendant invaded Plaintiffs' and Class Members' privacy by (a) intruding into their affairs in a manner that would be highly offensive to a reasonable person; (b) publicizing private facts about them, the publication of which would be highly offensive to a reasonable person; (c) appropriating and using their likeness without consent; and (d) violating their right to privacy, as guaranteed by the California Constitution, Article 1, Section 1, where Defendant obtained Plaintiffs' and Class Members' PII and/or otherwise allowed Plaintiffs' and Class Members' PII to be disclosed to unauthorized third parties.

72. Defendant knew or acted with reckless disregard to the fact that a reasonable person in Plaintiffs' and Class Members' position would consider Defendant's actions highly offensive.

73. Defendant invaded Plaintiffs' and Class Members' right to privacy and intruded into their private affairs by misusing and/or disclosing their PII without their informed, voluntary consent.

74. As a proximate result of such conduct, Plaintiffs' and Class Members' reasonable expectation of privacy in the above-described PII was unreasonably frustrated.

75. Defendant's conduct was wanton, engaged in with malice and oppression, and in conscious disregard of Plaintiffs' and Class Members' rights to have such PII kept private. As a result of the egregious nature of Defendant's behavior, Plaintiffs and Class Members' seek punitive damages individually and on behalf of the Class.

JURY DEMANDED

Pursuant to Federal Rule of Civil Procedure 38, Plaintiffs, individually and on behalf of the Class they seek to represent, demand a jury on any issue so triable of right by a jury.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, request judgment be entered against Defendant and that the Court grant the following:

1. An order determining that this action may be maintained as a class action under Rule 23 of the Federal Rules of Civil Procedure, that Plaintiffs are proper class representatives, that Plaintiffs' attorneys be appointed Class counsel pursuant to Rule 23(g) of the Federal Rules of Civil Procedure, and that Class notice be promptly issued;

2. Judgment against Defendant for Plaintiffs' and Class Members'

asserted causes of action;

3. Appropriate declaratory relief against Defendant;

4. Preliminary and permanent injunctive relief against Defendant;

5. An award of appropriate relief, including actual damages, restitution, disgorgement, and statutory damages pursuant to Cal. Civ. Code § 56.36, for $1,000 for each violation of Count Three;

6. An award of reasonable attorney's fees and other litigation costs reasonably incurred; and

7. Any and all relief to which Plaintiffs and the Class may be entitled.

Dated: December 18, 2014

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP

By: */s/ Michael W. Sobol*
Michael W. Sobol

Michael W. Sobol (State Bar No. 194857)
msobol@lchb.com
RoseMarie Maliekel (State Bar No. 276036)
rmaliekel@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: 415.956.1000
Facsimile: 415.956.1008

Nicholas Diamand
Pro Hac Vice forthcoming
ndiamand@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
250 Hudson Street, 8th Floor
New York, NY 10013-1413
Telephone: 212.355.9500
Facsimile: 212.355.9592

Hank Bates (State Bar No. 167688)
hbates@cbplaw.com
Allen Carney
acarney@cbplaw.com
David Slade
dslade@cbplaw.com
CARNEY BATES & PULLIAM, PLLC
11311 Arcade Drive
Little Rock, AR 72212
Telephone: 501.312.8500
Facsimile: 501.312.8505

Attorneys for Plaintiffs and the Proposed Class