

1 John H. Gomez (SBN 171485)
John P. Fiske (SBN 249256)
2 Stephanie S. Poli (SBN 286239)
GOMEZ TRIAL ATTORNEYS
3 655 West Broadway Suite1700
San Diego, CA 92101
4 Telephone: (619) 237-3490
Fax: (619) 237-3496

5 Attorneys for Plaintiff
6
7
8
9

10 **UNITED STATES DISTRICT COURT**
11 **CENTRAL DISTRICT OF CALIFORNIA – SOUTHERN DIVISION**

12 LAWON EXUM, individually and on
behalf of all others similarly situated,

13 PLAINTIFF,

14 v.

15 SONY PICTURES
16 ENTERTAINMENT, INC.,

17 DEFENDANT.
18
19
20

CASE NO. _____

CLASS ACTION COMPLAINT
FOR:

- 1) Violations of the California Records Act;
- 2) Violations of the California Unfair Competition Laws;
- 3) Violations of the Confidentiality of Medical Information Act; and
- 4) Negligence

JURY TRIAL DEMANDED

21 **CLASS ACTION COMPLAINT**

22 Plaintiff Lawon Exum (“Plaintiff”) files this class action complaint on behalf
23 of himself and all others similarly situated, by and through the undersigned attorneys,
24 against Defendant Sony Pictures Entertainment, Inc. (“Defendant” or “Sony
25 Pictures”) and alleges as follows upon personal knowledge as to himself and his own
26 acts and experiences and, as to all other matters, upon information and belief based
27 upon, *inter alia*, investigation conducted by his attorneys.
28

NATURE OF THE CASE

1
2 1. In or around November 2014, Sony Pictures suffered a massive data
3 breach of its corporate network whereby hackers gained access to sensitive and
4 confidential data available on the Sony Pictures corporate network, including full
5 names, home addresses, email addresses, password files, private key files, social
6 security numbers, dates of birth, bank account information, passport and other
7 personal identification information, retirement plan information, health insurance and
8 medical information, and other data.

9 2. The breach was a result of Sony Pictures' failure to develop, maintain,
10 and implement internet security measures on its corporate network. Sony Pictures'
11 serious lapses in industry standards regarding data protection measures have been
12 reported in various media outlets, many of which suggest that these lapses have been
13 ongoing for years.

14 3. Plaintiff, individually and on behalf of the Class defined below, seeks to
15 obtain relief from Defendant, including, *inter alia*, damages and declaratory relief,
16 based on Sony Pictures' failure to develop, implement, and maintain data security and
17 protection policies that were adequate, reasonable, and reflected industry standards.

JURISDICTION AND VENUE

18
19 4. This Court has subject matter jurisdiction of this action pursuant to 28
20 U.S.C. § 1332 because: (i) there are 100 or more class members, (ii) there is an
21 aggregate amount in controversy exceeding \$5,000,000, exclusive of interest and
22 costs, and (iii) there is minimal diversity because at least one plaintiff and defendant
23 are citizens of different states. This Court also has supplemental jurisdiction over
24 the state law claims pursuant to 28 U.S.C. § 1367.

25 5. Venue is proper in this judicial district and division pursuant to 28
26 U.S.C. § 1391 because Defendant is headquartered in this district and division, is
27 subject to personal jurisdiction in this district and division, and is thus deemed to be
28 a citizen of this district and division. Additionally, a substantial part of the events

1 and/or omissions giving rise to the claims occurred within this district and division.

2 6. This Court has personal jurisdiction over Defendant because it
3 maintains its principal place of business within this judicial district and division and
4 has such minimum contacts with California to make this Court's exercise of
5 jurisdiction proper.

6 **PARTIES**

7 7. Plaintiff Lawon Exum, a resident of the state of California, was
8 employed by Sony Pictures as a TV Legal File Clerk from January 2006 to June
9 2014. Plaintiff's personal information was compromised and released as a result of
10 the November 2014 data breach at Sony Pictures.

11 8. Defendant is a corporation duly organized and existing under the laws of
12 the State of Delaware with its headquarters and principal place of business located in
13 Los Angeles, California.

14 **FACTUAL ALLEGATIONS**

15 **The Attack on Defendant's Network**

16 9. On November 24, 2014, a number of media outlets issued reports of a
17 studio-wide cyberattack conducted by a group calling itself the "Guardians of Peace"
18 (or #GOP, as they refer to themselves). Sony Pictures was thereafter identified as the
19 subject of the attack. On December 19, 2014, the FBI confirmed that the government
20 of North Korea was responsible for the attack.¹

21 10. This is not the first time Sony has experienced such an attack. In 2011,
22 Sony's PlayStation Network was hit by one of the largest security breaches recorded,
23 in which approximately 77 million PlayStation accounts were hacked. On or about
24 June 6, 2011, Sony Pictures experienced a data breach whereby hackers called
25 "LulzSec" obtained over one million Sony customer passwords, phone numbers,
26 email addresses, home addresses, and birth dates. Despite this intimate familiarity,

27 ¹ <http://www.cnn.com/2014/12/19/politics/fbi-north-korea-responsible-sony/> (last
28 visited January 6, 2015).

1 Sony failed to improve its corporate network security in the three years since the
2 PlayStation and LulzSec hacks.

3 11. Upon gaining access to Sony Pictures' corporate network, access to all
4 of its phones, email-service, and computers was paralyzed. Further, it is believed the
5 text below was displayed on every computer on the network:

6 Hacked By #GOP

7 Warning:

8 We've already warned you, and this is just a beginning.

9 We continue till our request be met.

10 We've obtained all your internal data including your secrets and top secrets

11 If you don't obey us, we'll release data shown below to the world.

Determine what will you do till November the 24th, 11:00 PM (GMT).

12 12. Shortly after the display of the above messages, #GOP allegedly went on
13 to leak a number of unreleased Sony Pictures' films. Further, a self-titled "Boss of
14 GOP" began sending emails to media outlets that (a) claimed GOP was responsible
15 for the security breach and (b) that GOP was making the leaked films available
16 through peer-to-peer filesharing systems, such as BitTorrent.

17 13. The security breach was effectuated through the use of a malware
18 program that was capable of wiping memory, taking over total control of the system,
19 and accessing and transferring any data stored on the network.

20 14. Sony initially communicated that it was investigating an IT matter and
21 failed to disclose the breadth and severity of the catastrophic cyberattack on its
22 corporate networks.

23 15. The breach was not limited to Sony's own proprietary information.
24 Approximately one week after the initial attack, files were leaked that contained
25 personal and confidential information of more than 6,000 current and former Sony
26 employees. The files contained the pre-bonus salaries of the top 17 Sony executives,
27 as well as the salaries of thousands of other current and former employees.
28

1 16. On December 2, 2014, Brian Krebs of “Krebs on Security” reported that
2 more than 25 gigabytes of sensitive data on tens of thousands of Sony employees was
3 compromised and was being traded on BitTorrent networks and file-sharing websites
4 such as PasteBin.² This data included, at minimum, the following:

- 5 • Social security numbers;
- 6 • Medical information;
- 7 • Salary information;
- 8 • A global Sony employee list which contained the name, location,
9 employee ID, network username, base salary, and date of birth for more
10 than 6,800 individuals;
- 11 • April 2014 status report listing the names, dates of birth, SSNs and
12 health savings account data on more than 700 Sony employees; and
- 13 • Internal audit from accounting firm Pricewaterhouse Coopers, and
14 includes screen shots of dozens of employee federal tax records and
15 other compensation data.

16 17. On December 4, 2014, media outlets – including CNET – reported that
17 the social security numbers of more than 47,000 celebrities, freelancers, and current
18 and former Sony employees were released. Personal information, salaries, and home
19 addresses were also released.

20 18. On December 5, 2014, #GOP allegedly emailed numerous Sony
21 employees with the following threat:

22 Many things beyond imagination will happen at many places of the
23 world. Our agents find themselves act in necessary places. Please sign
24 your name to object the false of the company at the e-mail address
25 below if you don’t want to suffer damage. If you don’t, not only you
but your family will be in danger.³

26 ² See <http://krebsonsecurity.com/2014/12/sony-breach-may-have-exposed-employee-healthcare-salary-data/> (last visited January 6, 2015).

27 ³ See <http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interview->
28

1 19. On December 8, 2014, a list of celebrity aliases and contact information
2 was released.

3 20. On December 12, 2014, various media outlets reported that the stolen
4 documents released by #GOP included the medical records of Sony employees. A
5 separate document lists birth dates, health conditions, and medical costs incurred by
6 34 employees and their families.

7 21. On December 16, 2014, #GOP threatened to launch terrorist attacks at
8 movie theaters showing *The Interview* – a comedy film centered around a fictional
9 plot to kill North Korean leader Kim Jong-un that was scheduled for release on
10 Christmas Day. The premiere of *The Interview* was cancelled that same day. In
11 addition, thousands of of emails from Sony Pictures Co-Chairman and CEO Michael
12 Lynton were released.

13 22. On December 17, 2014, Sony Pictures canceled the release of *The*
14 *Interview* and all television advertising for the film. More private emails were also
15 leaked.

16 **Defendant Failed to Protect Confidential and Highly Sensitive Data**

17 23. Sony is no stranger to cyberattacks and data breaches. As noted above,
18 in 2011, Sony Computer Entertainment America LLC and Sony Network
19 Entertainment Internationa LLC suffered a data breach of its PlayStation network that
20 affected approximately 77 million users' personal information.

21 24. On or about June 6, 2011, Sony Pictures experienced a data breach
22 whereby hackers called "LulzSec" obtained over one million Sony customer
23 passwords, phone numbers, email addresses, home addresses, and birth dates. The
24 information stolen was allegedly unencrypted.⁴ It is unclear whether Sony Pictures
25 terminated any data security employees after this attack, or whether there were

26 north-korea-1201325501/ (last visited January 6, 2015).

27 ⁴ See <https://www.privacyrights.org/data-breach-asc?title=sony> (last visited January
28 6, 2015).

1 significant (or any) data protection and/or retention policy shifts that were
2 implemented.

3 25. In addition, data breaches and cyberattacks are becoming increasingly
4 more common, as evidenced by the recent widely publicized incidents at Target,
5 Home Depot, Michaels, Neiman Marcus, P.F. Chang's, Jimmy John's, and others.
6 As a result, companies that store and maintain confidential and highly sensitive
7 information must develop, implement, and maintain up-to-date data security and
8 retention policies that reduce the risk of cyberattack and unauthorized release of this
9 information.

10 26. Despite Defendant's own experiences, and its knowledge of recent data
11 breaches, it has failed to develop, implement, and maintain data security and retention
12 policies that reflect industry standards. In fact, an alleged Sony insider informed
13 Business Insider that "the security team has no f—king clue" what it's doing, and that
14 Sony's security policies were outdated and ineffective.

15 27. According to a former Sony employee, the company's information
16 security team is "a complete joke":

17 "We'd report security violations to them and our repeated reports were
18 ignored. For example, one of our Central European website managers
19 hired a company to run a contest, put it up on the TV network's website
20 and was collecting personally identifying information without encrypting
21 it. A hack of our file server about a year ago turned out to be another
22 employee in Europe who left himself logged into the network (and our
23 file server) in a cafe."⁵

24 28. Another former employee explains that Sony lacks any "real investment
25 in or real understanding of what information security is."⁶

26 ⁵ See <http://fusion.net/story/31469/sony-pictures-hack-was-a-long-time-coming-say-former-employees/> (last visited January 6, 2015).

27 ⁶ See <http://techcrunch.com/2014/12/16/hack-sony-twice-shame-on-sony/> (last visited
28 January 6, 2015).

1 29. Indeed, a number of notable internet security researchers have indicated
2 that Sony Pictures should have been able to detect unauthorized parties conducting
3 massive data copies in a systematic manner.⁷

4 30. Further evidencing Sony Pictures' primitive data protection and
5 retention policies, the files #GOP posted online show that Sony Pictures stored login
6 information for administrative accounts, social media accounts, and SSL certificates⁸
7 in a folder named "Password." The hackers used these passwords to cause further
8 damage and to release additional confidential and highly sensitive information.

9 31. An article published by the Associated Press identifies numerous flaws
10 in Sony Pictures' data security policies, including:

- 11 • Its chief executive was regularly reminded in unsecure emails of his own
12 secret passwords for his and his family's mail, banking, travel and
13 shopping accounts, according to a review of more than 32,000 stolen
14 corporate emails circulating on the Internet;
- 15 • Lax internet security practices inside Sony were prevalent, such as
16 pasting passwords into emails, using easy-to-guess passwords and failing
17 to encrypt especially sensitive materials such as confidential salary and
18 revenue figures, strategic plans and medical information about some
19 employees.
- 20 • In an October email, the company's chief financial officer, David C.
21 Hendler, complained to Lynton that Sony Pictures had experienced
22 months of "significant and repeated outages due to a lack of hardware
23 capacity, running out of disk space, software patches that impacted the
24 stability of the environment, poor system monitoring and an unskilled

25
26 ⁷ See <http://www.businessinsider.com/sony-insider-the-security-team-has-no-fing-clue-2014-12> (last visited January 6, 2015).

27 ⁸ SSL certificates digitally sign a web page to prove that it is actually from the
28 company.

1 support team.” Mr. Hendler also blamed a company rule that required
2 employees to keep too many old emails.

3 32. Kevin Mitnick – a former hacker who served five years in federal prison
4 and now runs a security consulting firm – described Sony Pictures’ approach as
5 sloppy. Mitnick noted that the lax password protection policy resulted in a much
6 more widespread and severe breach, as hackers who steal corporate data often
7 immediately search for the word “password” or a variation of the word across
8 thousands of messages.⁹

9 33. Sony Pictures failed to develop, implement, and maintain data security and
10 retention policies that would have both detected the breach and helped reduce the
11 severity or, potentially, would have prevented the breach entirely. This catastrophic
12 and complete failure by Sony Pictures resulted in increased exposure to data breaches
13 and caused the release of tens of thousands of current and former employees’
14 confidential, highly sensitive, and personal information onto the internet and
15 elsewhere.

16 34. To make matters worse, Sony Pictures has still failed to disseminate
17 adequate and detailed information to its current and former employees regarding the
18 breach, what data was in fact compromised and/or published, and what (if any)
19 measures Sony Pictures has undertaken to prevent identity theft and other fraudulent
20 conduct.

21 35. As a result of Sony Pictures’ failed policies and failure to announce or
22 implement any necessary identity theft, credit card fraud, or other-fraud based
23 services, Plaintiff and the members of the Class are at increased risk of being
24 subjected to stolen identities and fraudulent charges. Indeed, many members of the
25 Class have likely already had to cancel credit cards, pay for new credit cards to be

26 ⁹ See [http://www.apnewsarchive.com/2014/Sony-emails-reveal-loose-use-of-](http://www.apnewsarchive.com/2014/Sony-emails-reveal-loose-use-of-passwords-and-IDs-ripe-for-hacking/id-041c9dc46e9d408fa569ccac15c0ffe0)
27 [passwords-and-IDs-ripe-for-hacking/id-041c9dc46e9d408fa569ccac15c0ffe0](http://www.apnewsarchive.com/2014/Sony-emails-reveal-loose-use-of-passwords-and-IDs-ripe-for-hacking/id-041c9dc46e9d408fa569ccac15c0ffe0) (last
28 visited January 6, 2015).

1 issued, and pay for credit and identity theft monitoring services in order to prevent
2 further damage from the data breach.

3 **CLASS ACTION ALLEGATIONS**

4 36. Plaintiff brings this action on his own behalf, and on behalf of the
5 following Classes pursuant to FED. R. CIV. P. 23(a), 23(b)(2), and/or 23(b)(3).
6 Specifically, the Classes consist of each of the following:

7 **Nationwide Class:**

8 All residents of the United States who had their personal information
9 compromised as a result of the data breach of Sony Pictures' corporate
10 network.

11 Or, in the alternative,

12 **California Class:**

13 All residents of California who had their personal information
14 compromised as a result of the data breach of Sony Pictures' corporate
15 network.

16 37. Together, the Nationwide and California Classes shall be collectively
17 referred to herein as the "Class." Excluded from the Class are Defendant and the
18 Judge(s) assigned to this case. Plaintiff reserves the right to modify, change or
19 expand the Class definition after conducting discovery.

20 38. Numerosity: The Class is so numerous that joinder of all members is
21 impracticable. While the exact number and identities of individual members of the
22 Class are unknown at this time, such information being in the possession of
23 Defendant and obtainable by Plaintiff only through the discovery process, Plaintiff
24 believes that the Class consists of tens of thousands, if not hundreds, of current and
25 former Sony Pictures employees whose personal data was compromised.

26 39. Existence and Predominance of Common Questions of Fact and Law:
27 Common questions of law and fact exist as to all members of the Class. These
28 questions predominate over the questions affecting individual Class members. These

1 common legal and factual questions include, but are not limited to:

- 2 a. whether Defendant's data security and retention policies were
- 3 unreasonable;
- 4 b. whether Defendant failed to protect the confidential and highly
- 5 sensitive information of its current and former employees;
- 6 c. whether Defendant breached any legal duties in connection with the
- 7 November, 2014 data breach;
- 8 d. whether Defendant's conduct violated the California Customer
- 9 Records Act;
- 10 e. whether Defendant's conduct violated the Confidentiality of Medical
- 11 Information Act;
- 12 f. whether Defendant's conduct violated the California Unfair
- 13 Competition Law;
- 14 g. whether Defendant's constitutes actionable negligence;
- 15 h. whether Plaintiff and Class members are entitled to monetary
- 16 damages and/or other remedies and, if so, the nature of any such
- 17 relief; and
- 18 i. whether the Court may apply the law of the State of California to the
- 19 entire Class because Defendant's conduct emanated from California.

20 40. Typicality: All of Plaintiff's claims are typical of the claims of the

21 Class since Plaintiff and all members of the Class had their personal, confidential,

22 and highly sensitive information compromised in the November 2014 data breach.

23 41. Adequacy: Plaintiff is an adequate representative because his interests

24 do not materially or irreconcilably conflict with the interests of the Class that he

25 seeks to represent, he has retained counsel competent and highly experienced in

26 complex class action litigation, and he intends to prosecute this action vigorously.

27 The interests of the Class will be fairly and adequately protected by Plaintiff and his

28 counsel.

1 42. Superiority: A class action is superior to all other available means of
2 fair and efficient adjudication of the claims of Plaintiff and members of the Class.
3 The injury suffered by each individual Class member is relatively small in
4 comparison to the burden and expense of individual prosecution of the complex and
5 extensive litigation necessitated by Defendant's conduct. It would be virtually
6 impossible for members of the Class individually to effectively redress the wrongs
7 done to them. Even if the members of the Class could afford such individual
8 litigation, the court system could not. Individualized litigation presents a potential
9 for inconsistent or contradictory judgments. Individualized litigation increases the
10 delay and expense to all parties and to the court system presented by the complex
11 legal and factual issues of the case. By contrast, the class action device presents far
12 fewer management difficulties, and provides the benefits of single adjudication,
13 economy of scale, and comprehensive supervision by a single court. Members of the
14 Class can be readily identified and notified based on, *inter alia*, Defendant's records
15 and databases.

16 43. Defendant has acted, and refused to act, on grounds generally applicable
17 to the Class, thereby making appropriate final injunctive and equitable relief with
18 respect to the Class as a whole.

19 44. California's substantive laws may be constitutionally applied to the
20 claims of Plaintiff and the Nationwide Class under the Due Process Clause, 14th
21 Amend., § 1, and the Full Faith and Credit Clause, art. IV., § 1, of the U.S.
22 Constitution. California has significant contact, or significant aggregation of
23 contacts, to the claims asserted by Plaintiff and all Class members, thereby creating
24 state interests that ensure that the choice of California state law is not arbitrary or
25 unfair. Specifically, Defendant's headquarters and principal place of business are
26 located in California, and upon information and belief, the conduct that gave rise to
27 Plaintiff's claims emanated from California.

28 ///

VIOLATIONS ALLEGED

COUNT I

VIOLATIONS OF THE CALIFORNIA CUSTOMER RECORDS ACT

(CAL. CIV. CODE § 1798.80, *et seq.*)

(On Behalf of the Nationwide Class or, Alternatively, the California Class)

45. Plaintiff re-alleges and incorporates by reference the allegations contained in all preceding paragraphs of this Complaint as though set forth fully herein.

46. Sony Pictures is a “business” as that term is defined in Cal. Civ. Code § 1798.80(a).

47. Plaintiff and the Class members are “individual[s]” as that term is defined in Cal. Civ. Code § 1798.80(d).

48. Plaintiff and the Class members had “personal information” compromised as a result of the November 2014 data breach, as that term is used in both Cal. Civ. Code 1798.80(e) and 1798.81.5(d)(1)(C).

49. The data breach of Sony Pictures’ corporate network in November 2014 constitutes a “breach of the security system” pursuant to Cal. Civ. Code § 1798.82(g).

50. Sony Pictures’ policies and procedures regarding data protection and retention violated Cal. Civ. Code § 1798.81.5, as Sony Pictures’ measures were unreasonable and wholly failed to prevent access to, and disclosure of, its current and former employees’ personal information.

51. Sony Pictures also violated Cal. Civ. Code § 1798.82 by failing to notify Plaintiff and the Class members that their personal, confidential, and highly sensitive information had been compromised and/or stolen by hackers.

52. As a result of Sony Pictures’ conduct as described herein, Plaintiff and the Class members have been injured

53. Plaintiff seeks monetary damages, including damages related to the acquisition of identity theft and credit monitoring services, injunctive and declaratory relief pursuant to Cal. Civ. Code § 1798.84(e), and attorneys' fees and costs.

COUNT II
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW,
BUSINESS AND PROFESSIONS CODE § 17200, *et seq.*
(On Behalf of the Nationwide Class or, Alternatively, the California Class)

54. Plaintiff re-alleges and incorporates by reference the allegations contained in all preceding paragraphs of this Complaint as though set forth fully herein.

55. California Business & Professions Code § 17200, *et seq.* prohibits acts of "unfair competition", which is defined by Business & Professions Code § 17200 as including any "any unlawful, unfair or fraudulent business act or practice"

56. Sony Pictures' conduct constitutes unlawful and unfair practices because it constitutes violations of Cal. Civ. Code § 1798.80, *et seq.*, the Confidentiality of Medical Information Act, the Health Insurance Portability and Accountability Act of 1996, as well as actionable negligence.

57. Sony Pictures' conduct was unlawful as it failed to design, implement, and maintain reasonable security measures in protecting the personal, confidential, and highly sensitive data of its current and former employees, including medical information protected by the CMIA and HIPAA, as well as by failing to timely notify Plaintiff and the Class about the data breach.

58. Plaintiff and the Class members have suffered injuries as a direct and proximate result of Sony Pictures' acts as alleged herein. Plaintiff and the Class have suffered damages through the purchase of credit and identity theft monitoring service, as well as through the cancelling of credit cards and bank accounts, and the fees associated therewith, as well as the time invested by Plaintiff and the Class in protecting themselves from identity theft and other fraud as a result of Sony Pictures'

1 breaches, in addition to the risk for future identity theft and fraudulent activity.

2 59. Plaintiff seeks to enjoin further unlawful, unfair and/or fraudulent acts
3 or practices by Defendant, and all other relief allowed under CAL. BUS. & PROF.
4 CODE § 17200.

5 **COUNT III**
6 **VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL**
7 **INFORMATION ACT (CAL. CIV. CODE § 56, *et seq.*)**
8 **(On Behalf of the Nationwide Class)**

9 60. Plaintiff re-alleges and incorporates by reference the allegations
10 contained in all preceding paragraphs of this Complaint as though set forth fully
11 herein.

12 61. CAL. CIV. CODE § 56, *et seq.*, requires employers that receive medical
13 information from employees or patients to design, implement, and maintain
14 procedures to ensure the confidentiality and protection from unauthorized use and
15 disclosure of such information. CAL. CIV. CODE § 56 also prohibits employers from
16 the disclosure of medical information without first obtaining written authorization.

17 62. Sony Pictures was in the possession of, and retained, medical records
18 belonging to, and regarding, its current and former employees.

19 63. CAL. CIV. CODE § 56, *et seq.*, imposed a legal duty on Sony Pictures to
20 protect the confidential and highly sensitive medical information of Plaintiff and the
21 Class.

22 64. Sony Pictures failed to develop, implement, and maintain data security and
23 retention policies that would have prevented the access to Plaintiff and the Class's
24 medical information without prior written authorization. As such, Sony Pictures
25 violated the legal duty imposed on it by CAL. CIV. CODE § 56, *et seq.*

26 65. CAL. CIV. CODE § 56.36 entitles Plaintiff and the Class who had medical
27 information compromised during the data breach to \$1,000 per class member as well
28 as actual damages.

COUNT IV
NEGLIGENCE

(On Behalf of the Nationwide Class or, Alternatively, the California Class)

66. Plaintiff re-alleges and incorporates by reference the allegations contained in all preceding paragraphs of this Complaint as though set forth fully herein.

67. Sony Pictures owed Plaintiff and the Class a duty to exercise reasonable care in the retention and protection of Plaintiff's and the Class' personal, confidential, and highly sensitive information. This duty included the development, implementation, and maintenance of policies and procedures that would protect Plaintiff's and the Class' personal, confidential, and highly sensitive information from access by unauthorized third parties and persons. Sony Pictures was also aware of its inadequate data protection and retention policies because it was subject to a data breach that revealed personal and confidential information just three years prior.

68. Sony Pictures also owed Plaintiff and the Class a duty to notify them, within a reasonable time, of the data breach that occurred in November 2014 and provide a comprehensive list that detailed, *inter alia*, what information was compromised in the attack. This failure has prevented members of the Class to take the necessary measures to avoid further damages from the data breach, including, *inter alia*, credit and identity theft monitoring services for persons whose information was disclosed.

69. Sony Pictures knew, or should have known, of the level of data security required to protect the information it was collecting and retaining from its current and former employees.

70. Sony Pictures' failure to develop, implement, and maintain adequate data collection, retention, and protection policies created a risk of harm to Plaintiff and the Class that was foreseeable. Sony Pictures knew, or should have known, that

1 its data collection, retention, and protection policies were unreasonable and did not
 2 reflect industry standards, in part because Sony Pictures suffered a data breach just
 3 three years prior to the November 2014 data breach.

4 71. Sony Pictures breached its duties owed to Plaintiff and the Class. As a
 5 direct and proximate result of Sony Pictures' breach, Plaintiff and the Class' personal,
 6 confidential, and highly sensitive information was breached from Sony Pictures'
 7 corporate network and disseminated without their knowledge or consent. This has
 8 caused Plaintiff and the Class damages through the purchase of credit and identity
 9 theft monitoring service, as well as through the cancelling of credit cards and bank
 10 accounts, and the fees associated therewith, as well as the time invested by Plaintiff
 11 and the Class in protecting themselves from identity theft and other fraud as a result
 12 of Sony Pictures' breaches, in addition to the risk for future identity theft and
 13 fraudulent activity.

14 **PRAYER FOR RELIEF**

15 WHEREFORE, Plaintiff, on behalf of himself and members of the Class,
 16 respectfully requests that this Court:

- 17 A. Determine that the claims alleged herein may be maintained as a class
 18 action under Rule 23 of the Federal Rules of Civil Procedure, and issue
 19 an order certifying one or more Classes as defined above;
- 20 B. Appoint Plaintiff as the representative of the Class and his counsel as
 21 Class counsel;
- 22 C. Award all actual, general, special, incidental, statutory, and
 23 consequential damages to which Plaintiff and Class members are
 24 entitled;
- 25 D. Award pre-judgment and post-judgment interest on such monetary
 26 relief;
- 27 E. Grant appropriate injunctive and/or declaratory relief;
- 28 F. Award reasonable attorneys' fees and costs; and

1 G. Grant such further relief that this Court deems appropriate.

2
3 **DEMAND FOR JURY TRIAL**

4 Plaintiff respectfully demands a trial by jury on all issues so triable.

5
6 Dated: January 6, 2015

Respectfully submitted,

7
8 By: /s/ John P. Fiske

9 John H. Gomez, Esq.
John P. Fiske, Esq.
10 **GOMEZ TRIAL ATTORNEYS**
655 West Broadway Suite 1700
11 San Diego, CA 92101
Telephone: (619) 237-3490
12 Fax: (619) 237-3496

13 Katrina Carroll (To Apply *Pro Hac Vice*)
14 Kyle A. Shamberg (To Apply *Pro Hac Vice*)
LITE DEPALMA GREENBERG, LLC
211 W. Wacker Drive Suite 500
15 Chicago, IL 60613
(312) 750-1265
16 kcarroll@litedepalma.com
17 kshamberg@litedepalma.com
18
19
20
21
22
23
24
25
26
27
28