

02:04:48 p.m. 02-24-2015 11

FEB/24/2015/TUE 03:15 PM

FAX No.

P. 011

1 BLOOD HURST & O'REARDON, LLP
 2 TIMOTHY G. BLOOD (149343)
 3 THOMAS J. O'REARDON II (247952)
 4 701 B Street, Suite 1700
 5 San Diego, CA 92101
 6 Tel: 619/338-1100
 7 619/338-1101 (fax)
 8 tblood@bholaw.com
 9 toreardon@bholaw.com

*WJD
6/20/15*

FILED
Superior Court of California
County of Los Angeles

FEB 24 2015

Sherril R. Carter, Executive Officer/Clerk
By [Signature] Deputy
Shaunya Bolden

6 Attorneys for Plaintiffs and the Putative Class
7 [Additional Counsel Appear on Signature Page]

*307 Hojue
AM*

**SUPERIOR COURT OF THE STATE OF CALIFORNIA
COUNTY OF LOS ANGELES -STANLEY MOSK COURTHOUSE**

BLOOD HURST & O'REARDON, LLP

11 BRUCE OCHMANEK and HIRAM A.
12 VARGAS, on behalf of themselves and all
13 others similarly situated,

13 Plaintiffs,

14 v.

15 SONY PICTURES ENTERTAINMENT,
16 INC.,

16 Defendant.

Case No.

CLASS ACTION **BC 5 7 3 3 6 6**

CLASS ACTION COMPLAINT

BY FAX

JURY TRIAL DEMANDED

CIT/CASE: BC573366
 LGN/DEF#: _____
 RECEIPT #: CCH481620041
 DATE PAID: 02/25/15 11:07 AM
 PAYMENT: \$1,435.00 \$18
 RECEIVED:
 CHECK: \$0.00
 CASH: \$0.00
 CHANGE: \$0.00
 CARD: \$1,435.00

Case No

1 Plaintiffs Bruce Ochmanek and Hiram A. Vargas (together, "Plaintiffs"), on behalf of
2 themselves and all others similarly situated, bring this action against Defendant Sony Pictures
3 Entertainment, Inc. ("Sony", "SPE" or "Defendant"), and respectfully allege the following:

4 **NATURE OF THE ACTION**

5 1. This is an employment and data breach case. Plaintiffs, individually and on
6 behalf of over 47,000 similarly situated persons (*i.e.*, the Class Members), bring this class
7 action based solely on California law to secure redress for Sony's intentional, willful and
8 reckless violations of their employment and privacy rights. Plaintiffs and Class Members are
9 current and former Sony employees and independent contractors who entrusted their
10 personally identifiable information ("PII") and medical records and private health information
11 ("PHI") (together, "PII/PHI") to Sony.

12 2. In November 2014, Sony betrayed Plaintiffs' and Class Members' trust by
13 failing to properly safeguard and protect their PII/PHI, thereby publicly disclosing their
14 PII/PHI without authorization (*i.e.*, the "Data Breach" or "Breach") in violation of numerous
15 laws, including, *inter alia*, the California Confidentiality of Medical Information Act
16 ("CMIA") (CAL. CIV. CODE § 56, *et seq.*), California Unfair Competition Law (CAL. BUS. &
17 PROF. CODE § 17200, *et seq.*), California Security Requirements for Consumer Records (CAL.
18 CIV. CODE §§ 1798.29 and 1798.80, *et seq.*), California Labor Code §§ 2800 and 2802
19 (indemnification), and California common law.

20 3. On or about December 2, 2014, after reports began surfacing on the Internet,
21 Sony announced that on November 24, 2014, it learned that Plaintiffs' and Class Members'
22 PII/PHI had been unlawfully released, disclosed, and disseminated to the world without their
23 authorization (*i.e.*, the "Data Breach").

24 4. The wrongfully released and disclosed PII/PHI included, *inter alia*, Plaintiffs'
25 and Class Members' (i) names, (ii) addresses, (iii) Social Security numbers, driver license
26 numbers, passport numbers, or other government identifiers, (iv) bank account information, (v)
27 credit card information for corporate travel and expense, (vi) usernames and passwords, (vii)
28 compensation, (viii) other employment-related information, (ix) HIPAA-protected health

1 information, such as names, Social Security numbers, claims appeals information submitted to
2 Sony (including diagnoses and disability codes), dates of birth, home addresses, and Sony
3 health plan member ID numbers, and (x) health/medical information provided to Sony outside
4 of the Sony health plans. In a December 8, 2014 Data Breach Notification Letter (Exhibit A),
5 Sony confirmed to Plaintiffs and Class Members the above-referenced information had been
6 released and disclosed without their authorization.

7 5. Sony flagrantly disregarded Plaintiffs' and Class Members' privacy rights by
8 intentionally, willfully, and recklessly failing to take the necessary precautions required to
9 safeguard and protect their PII/PHI from unauthorized disclosure. On information and belief,
10 Plaintiffs' and Class Members' PII/PHI was improperly handled and stored, either
11 unencrypted or improperly partially encrypted, unprotected, readily able to be copied by data
12 thieves, and not kept in accordance with basic security protocols. As described in greater
13 detail below, the wrongfully released and disclosed PII/PHI was transferred, sold, opened,
14 read, mined or otherwise used without Plaintiffs' and Class Members' authorization.

15 6. Sony's wrongful actions, inaction, omissions, want of ordinary care, and
16 intentional, willful and reckless disregard of Plaintiffs' and Class Members' employment and
17 privacy rights which, on information and belief, occurred entirely within the State of
18 California, directly or proximately caused the Data Breach and the unauthorized dissemination
19 of their PII/PHI to the world.

20 7. Plaintiffs are concerned about their finances, credit, identities, medical records,
21 and PII/PHI and, as such, regularly monitor their credit, regularly monitor their financial
22 accounts or carefully store and dispose of their PII/PHI and other documents containing their
23 PII/PHI. Since the Data Breach, Plaintiffs and Class Members have experienced identity
24 theft,¹ identity fraud, medical fraud,² lost medical identities and records, fraudulent credit card
25

26 _____
27 ¹ According to the United States Government Accounting Office (GAO), the terms
28 "identity theft" or "identity fraud" are broad terms encompassing various types of criminal
activities. Identity theft occurs when PII/PHI is used to commit fraud or other crimes. These
crimes include, *inter alia*, credit card fraud, phone or utilities fraud, bank fraud and
government fraud (theft of government services, including medical services).

1 activity, the opening or re-opening of new credit card accounts in their name, phishing scams,³
 2 increased mailers marketing products and services including, *inter alia*, medical products,
 3 medical services or prescription drugs specifically targeted to their medical conditions, and the
 4 imminent, immediate or continuing increased risk of identity theft, identity fraud or medical
 5 fraud.

6 8. Plaintiffs have standing to bring this suit because as a direct and proximate
 7 result of Sony's wrongful actions, inaction, omissions, and want of ordinary care, and the
 8 resulting Data Breach, they have suffered (and will continue to suffer) economic damages and
 9 other injury and actual harm in the form of, *inter alia*, (i) actual identity theft, identity fraud or
 10 medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv)
 11 statutory nominal damages of \$1000 per Plaintiff and each Class Member under the CMIA
 12 (CAL. CIV. CODE § 56.36(b)(1)), (v) expenses and losses in discharging their duties (CAL. LAB.
 13 CODE §§ 2800 and 2802), (vi) deprivation of the value of their PII/PHI, for which there is a
 14 well-established national and international market,⁴ (vii) the financial and temporal cost of

15
 16 ² Medical fraud (or medical identity theft) occurs when a data thief uses a victim's name
 17 or health insurance numbers to see a doctor, get prescription drugs, file claims with insurance
 18 providers, or obtain other medical care. *See* [http://www.consumer.ftc.gov/articles/0171-](http://www.consumer.ftc.gov/articles/0171-medical-identity-theft)
 19 [medical-identity-theft](http://www.consumer.ftc.gov/articles/0171-medical-identity-theft) (last visited August 10, 2014). If the thief's health information is mixed
 20 with the victim's information, the victim's medical treatment, insurance and payment records,
 21 and credit report may be affected. *Id.*

22 ³ "Phishing" is an attempt to acquire information (and sometimes, indirectly, money),
 23 such as usernames, passwords and credit card details by masquerading as a trustworthy entity
 24 through an electronic communication. Communications purporting to be from popular social
 25 websites, auction sites, online payment processors or IT administrators are commonly used to
 26 lure the unsuspecting public. Phishing emails may contain links to websites that are infected
 27 with malware. Phishing is typically carried out by e-mail spoofing or instant messaging, and
 28 often directs users to enter details at a fake website that looks and feels almost identical to the
 legitimate one. When criminals have access to PII/PHI from a large group of similarly situated
 victims, it is much more feasible to develop a believable phishing spoof email that appears
 realistic. They can then get this group of victims to reveal additional private information, such
 as credit cards, bank accounts, and the like.

⁴ PII/PHI is a valuable property right. *See, e.g.,* John T. Soma, *et al*, *Corporate Privacy*
 25 *Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of*
 26 *Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-*4 (2009) ("PII, which companies obtain at
 27 little cost, has quantifiable value that is rapidly reaching a level comparable to the value of
 28 traditional financial assets.") (citations omitted). It is so valuable to identity thieves that once
 PII has been compromised, criminals often trade it on the "cyber black-market" for several
 years.

Theft of PHI is also gravely serious; to wit, "[a] thief may use your name or health
 insurance numbers to see a doctor, get prescription drugs, file claims with your insurance

1 monitoring their credit, monitoring their financial accounts, and mitigating their damages (*see*
2 below), and (viii) the imminent, immediate and continuing increased risk of identity theft,
3 identity fraud or medical fraud – for which they are entitled to compensation.

4 9. Plaintiffs, on behalf of themselves and the other Class Members, seek (i) actual
5 and other economic damages, consequential damages, nominal damages, and statutory
6 damages, (ii) civil penalties, (iii) punitive damages, (iv) equitable relief, (v) injunctive relief,
7 and (vi) attorneys' fees, litigation expenses and costs.

8 JURISDICTION AND VENUE

9 10. This Court has jurisdiction over this matter pursuant to the California
10 Constitution, Article XI, § 10 and California Code of Civil Procedure ("CCP") § 410.10,
11 because Defendant transacted business and committed the acts alleged in California. More
12 than two-thirds of the Class Members are citizens and residents of California, the sole
13 defendant is located in California, and Defendant has its principal place of business in and is
14 headquartered in California; thus, this case is not subject to removal under the Class Action
15 Fairness Act of 2005 under both the "home state exception" and the "local controversy
16 exception." 28 U.S.C. § 1332(d)(4)(A) (home state exception); 28 U.S.C. § 1332 (d)(4)(B)
17 (local controversy exception).

18
19
20
21 provider, or get other care. If the thief's health information is mixed with yours, your
22 treatment, insurance and payment records, and credit report may be affected." *See* Federal
23 Trade Commission, *Medical Identity Theft*, [http://www.consumer.ftc.gov/articles/0171-](http://www.consumer.ftc.gov/articles/0171-medical-identity-theft)
24 [medical-identity-theft](http://www.consumer.ftc.gov/articles/0171-medical-identity-theft) (last visited March 27, 2014). Drug manufacturers, medical device
25 manufacturers, pharmacies, hospitals and other healthcare service providers often purchase
26 PII/PHI on the black market for the purpose of target marketing their products and services to
27 the physical maladies of the data breach victims themselves. Insurance companies purchase
28 and use compromised PHI to adjust their insureds' medical insurance premiums.

25 The value of PHI as a commodity also is measurable. *See, e.g.,* Robert Lowes, *Stolen*
26 *EHR [Electronic Health Record] Charts Sell for \$50 Each on Black Market* (April 28, 2014),
27 <http://www.medscape.com/viewarticle/824192> (last visited June 26, 2014); Adam Greenberg,
28 *Health Insurance Credentials Fetch High Prices in the Online Black Market* (July 16, 2013)
(all-inclusive health insurance dossiers containing sensitive health insurance information,
names, addresses, telephone numbers, email addresses, Social Security numbers and bank
account information, complete with account and routing numbers, are fetching \$1,200 to
\$1,300 each), [http://www.scmagazine.com/health-insurance-credentials-fetch-high-prices-in-](http://www.scmagazine.com/health-insurance-credentials-fetch-high-prices-in-the-online-black-market/article/303302/)
[the-online-black-market/article/303302/](http://www.scmagazine.com/health-insurance-credentials-fetch-high-prices-in-the-online-black-market/article/303302/) (last visited June 26, 2014).

1 11. Venue is appropriate in Los Angeles County because Plaintiffs reside in Los
 2 Angeles County and Defendant, which is headquartered in Los Angeles County, did and is
 3 doing business in Los Angeles County.

4 **PARTIES**

5 12. Plaintiff Bruce Ochmanek (“Ochmanek”) is a citizen and resident of Los
 6 Angeles, California, who previously was employed by Sony. As a result, Ochmanek entrusted
 7 Sony with his most sensitive personal and medical information (*i.e.*, his PII/PHI) which,
 8 pursuant to law, Sony was (and continues to be) required to safeguard, protect, and keep
 9 confidential. Sony, however, failed to do so, which Sony confirmed to Ochmanek in its Data
 10 Breach Notification Letter. In the letter, Sony confirmed that his PII/PHI was stored on the
 11 unprotected server hacked by the group known as “Guardians of Peace” on or about November
 12 24, 2014, and exposed to the world. Thereafter, one or more data thieves and their subsequent
 13 customers transferred, sold, opened, read, mined and otherwise used Ochmanek’s PII/PHI,
 14 without his authorization, to their financial benefit and his financial detriment. Since the Data
 15 Breach, Ochmanek has spent numerous hours monitoring his credit and financial accounts for
 16 fraudulent activity. As a direct and proximate result of Sony’s wrongful actions, inaction,
 17 omissions, and want of ordinary care, and the resulting Data Breach, Ochmanek has suffered
 18 (and will continue to suffer) the above-described economic damages and other injury and
 19 actual harm. Sony’s unauthorized and wrongful release and disclosure of Ochmanek’s PII/PHI
 20 also placed him at an imminent, immediate, and continuing increased risk of injury and harm
 21 from identity theft, identity fraud, and medical fraud.

22 13. Plaintiff Hiram A. Vargas (“Vargas”) is a citizen and resident of Los Angeles,
 23 California, who was employed by Sony until February 26, 2014. As a result, Vargas entrusted
 24 Sony with his most sensitive personal and medical information (*i.e.*, his PII/PHI) which,
 25 pursuant to law, Sony was (and continues to be) required to safeguard, protect, and keep
 26 confidential. Sony, however, failed to do so, which Sony confirmed to Vargas in its Data
 27 Breach Notification Letter. In the letter, Sony confirmed that his PII/PHI was stored on the
 28 unprotected server hacked by the group known as “Guardians of Peace” on or about November

1 24, 2014, and exposed to the world. Thereafter, one or more data thieves or their subsequent
2 customers transferred, sold, opened, read, mined or otherwise used Vargas' PII/PHI, without
3 his authorization, to their financial benefit and his financial detriment. Since the Data Breach,
4 Vargas has spent numerous hours monitoring his credit and financial accounts for fraudulent
5 activity. As a direct and proximate result of Sony's wrongful actions, inaction, omissions, and
6 want of ordinary care, and the resulting Data Breach, Vargas has suffered (and will continue to
7 suffer) the above-described economic damages and other injury and actual harm. Sony's
8 unauthorized and wrongful release and disclosure of Vargas' PII/PHI also placed him at an
9 imminent, immediate, and continuing increased risk of injury and harm from identity theft,
10 identity fraud, and medical fraud.

11 14. Defendant Sony Pictures Entertainment, Inc. ("SPE") is a Delaware corporation
12 with its principal place of business in Culver City, California. SPE is the wholly-owned
13 entertainment subsidiary of Sony Corporation of America. Based in Culver City, California, it
14 encompasses Sony's motion picture, television production, and distribution units. SPE's gross
15 revenue for the fiscal year ended March 31, 2014 has been reported to be approximately \$8
16 billion. Throughout the years, SPE has produced, distributed, or co-distributed successful
17 motion picture franchises, such as *Spider-Man*, *Men in Black*, *Underworld*, and *Resident Evil*.
18 At all relevant times, SPE maintained the internal computer systems and network breached in
19 the Data Breach and, therefore, was (and continues to be) obligated to safeguard and protect
20 Plaintiffs' and Class Members' PII/PHI – which it failed to do. As set forth in detail below,
21 SPE's wrongful actions, inaction, omissions, want of ordinary care, and intentional, willful and
22 reckless disregard of Plaintiffs' and Class Members' employment and privacy rights –
23 including openly storing thousands of passwords in a folder named "Password" and failing to
24 encrypt Plaintiffs' and Class Members' PII/PHI – which, on information and belief, occurred
25 entirely within the State of California, form a significant basis for Plaintiffs' and Class
26 Members' claims. As such, Plaintiffs and Class Members seek to recover significant relief
27 from Sony Pictures for their economic damages and other injury and actual harm inflicted on
28 them within the State of California.

FACTS

A. The Data Breach Released and Disclosed Plaintiffs’ and Class Members’ PII/PHI Without Their Authorization

15. On November 24, 2014, hackers calling themselves the Guardians of Peace infiltrated and disrupted Sony’s internal computer systems and networks (the “Data Breach”), warning Sony they intended to post “secrets” on the Internet they had obtained in the Data Breach.

16. Thereafter, on December 2, 2014, the Guardians of Peace carried out their threat, initially publishing Plaintiffs’ and Class Members’ PII/PHI online – including their names, Social Security numbers, birthdates, home addresses, job titles, performance evaluations, scans of passports and visas, compensation, reasons for termination, and details of severance packages.

17. Also on December 2, 2014, noted data security blogger Brian Krebs initially reported on his website, Krebs on Security (www.krebsonsecurity.com), that the hackers had obtained more than 25 gigabytes of sensitive data on tens of thousands of Sony current and former employees and independent contractors (*i.e.*, Plaintiffs and Class Members), including Social Security numbers, medical information (PHI) and salary information. *See* <http://krebsonsecurity.com/page/3/> (last visited January 2, 2015). Krebs noted that the hackers also may have destroyed data on an unknown number of Sony’s internal computer systems and networks. *Id.*

18. Krebs further reported that he had discovered several files being actively traded on torrent networks, such as pastebin.com, including a global Sony employee list, a Microsoft Excel file containing the names, locations, employee ID numbers, network usernames, base salaries, and dates of birth for more than 6,800 individuals. *Id.* Another file actively traded online was an April 2014 status report listing the names, dates of birth, Social Security numbers, and health savings account data on more than 700 Sony employees. *Id.* Yet another traded file was the product of an internal audit performed by Pricewaterhouse Coopers that

1 includes screen shots of dozens of Sony employee federal tax records and other compensation
2 data. *Id.*

3 19. On December 5, 2014, Sony reported the Data Breach had released and
4 disclosed more of its current and former employees' and independent contractors' PII/PHI than
5 originally thought. The updated tally was 47,426 unauthorized disclosures of unique names,
6 Social Security numbers, dates of birth, home addresses, email addresses, and salary
7 information of more than 15,200 current and former Sony employees and independent
8 contractors. The Social Security numbers were copied more than 1.1 million times throughout
9 the 601 files obtained by the hackers according to Identity Finder, LLC, which analyzed the
10 PII/PHI released and disclosed in the Data Breach. None of the PII/PHI, which also was
11 posted online on multiple file sharing websites, was protected by passwords.

12 20. Also on December 5, 2014, the hackers were reported to have sent an email to
13 numerous Sony current and former employees and independent contractors threatening them
14 and their families with "danger" if they did not support the Guardians of Peace and their
15 actions.

16 21. As of December 8, 2014, approximately 140 gigabytes out of at least 100
17 terabytes of internal Sony files, films, and information the hackers claim to possess – *i.e.*,
18 approximately ten times the amount of information stored in the Library of Congress – had
19 been released and disclosed on the Internet. On information and belief, the Class and its
20 damages will continue to grow in size as more compromised PII/PHI is published, bought,
21 sold, and traded on the Internet without authorization, and utilized to commit identity and
22 medical fraud.

23 **B. Sony's Data Breach Notification Letters and Offered "Remedy" Are Woefully**
24 **Deficient**

25 22. On December 8, 2014, Sony formally notified Plaintiffs and Class Members
26 about the Data Breach, confirming that the security of their PII/PHI and their dependents'
27 PII/PHI that Sony received from them during the course of their employment – including: (i)
28 names, (ii) addresses, (iii) Social Security numbers, driver license numbers, passport numbers,

1 or other government identifiers, (iv) bank account information, (v) credit card information for
2 corporate travel and expense, (vi) usernames and passwords, (vii) compensation, and (viii)
3 other employment-related information – had been released, disclosed, and compromised
4 without their authorization as part of the Data Breach. *Id.* See exemplar of uniform December
5 8, 2014 Data Breach Notification Letter sent to Plaintiffs and Class Members (Exhibit A).

6 23. Sony also confirmed in the Data Breach Notification Letter that Plaintiffs’ and
7 Class Members’ PHI – including: (i) HIPAA-protected health information, such as names,
8 Social Security numbers, claims appeals information submitted to Sony (including diagnoses
9 and disability codes), dates of birth, home addresses, and Sony health plan member ID
10 numbers, and (ii) health/medical information provided to Sony outside of the Sony health
11 plans – had been released, disclosed, and compromised without their authorization as part of
12 the Data Breach.. *Id.*

13 24. The Data Breach Notification Letters are materially misleading.
14 Notwithstanding the publication and active trading of Plaintiffs’ and Class Members’ PII/PHI
15 on black market websites, the Data Breach Notification Letters, which are uniform except for
16 the addressees, advised the recipients that their PII/PHI “*may* have been compromised” in the
17 Data Breach. *Id.* (emphasis added). The Data Breach Notification Letters also failed to
18 explain the breadth of the Data Breach, how it occurred, and why their PII/PHI was not
19 properly safeguarded and protected. Nor did Sony explain any steps being taken to protect
20 against future unauthorized disclosures of their PII/PHI.

21 25. The Data Breach Notification Letters also squarely placed the burden on
22 Plaintiffs and Class Members, rather than Sony, to protect themselves and mitigate their Data
23 Breach damages – such as reviewing their account statements, monitoring their credit reports,
24 and changing their passwords. *Id.* Unfortunately, many of Sony’s mitigation suggestions
25 required Plaintiffs and Class Members to incur additional out-of-pocket expenses. For
26 example, as a general rule in California, the fee to place (and remove) a “security freeze” on
27 one’s credit report, as suggested by the Data Breach Notification Letters, is \$10 each time it is
28 placed at each of the three credit reporting agencies (Experian, Equifax, and TransUnion).

1 Monitoring one's credit reports, another option suggested by the Data Breach Notification
2 Letters, would cause a Data Breach victim to incur an expense to see his or her credit reports
3 beyond the one free annual report to which they are entitled.

4 26. Sony's wrongful actions, inaction, omissions, and want of ordinary care in
5 failing to completely and accurately notify Plaintiffs and Class Members about the Data
6 Breach and corresponding unauthorized release and disclosure of their PII/PHI were arbitrary,
7 capricious and in derogation of Sony's duties to Plaintiffs and Class Members and the
8 notification procedures required by California law.

9 27. The Data Breach Notification Letters also notified Plaintiffs and Class
10 Members that Sony would provide one year of free credit monitoring and identity theft
11 insurance to all affected persons who take more time away from their businesses and families
12 to enroll. The offered "data security package," however, is inadequate. At best, the credit
13 monitoring service is an indirect manner of tracking identity theft – it may reveal new credit
14 accounts opened with compromised PII/PHI, but does nothing to prevent unauthorized charges
15 made to existing payment card accounts. The PII/PHI "protection" offered by Sony also is
16 woefully inadequate because, *inter alia*:

- 17 (i) The free credit monitoring and identity theft insurance was offered by Sony for
18 only one year. As advised by the Federal Trade Commission, however, a
19 person impacted by a data breach should take proactive steps well after a year
20 has passed to protect against identity theft and related risks as experts have
21 found that fraudsters typically hold purloined PII/PHI for over a year before
22 using it or re-selling it;
- 23 (ii) Sony offered only a single bureau credit monitoring program – as opposed to
24 the industry recommended triple bureau program – that provides no protection
25 to minors. Each minor child victim continues to be fully exposed to damages;
26 and
- 27 (iii) Sony did not provide any protection against medical identity theft and
28 fraudulent health insurance claims, the victims of which are often left with huge
medical bills, damaged credit, public disclosure of their medical condition and
erroneous medical records. According to a September 2011 report by PwC's
Health Resource Institute "Old Data Learns New Tricks," the problem of
medical identity theft is worsening and is the fastest growing form of identity
theft. Old Data Learns New Tricks, *available at* [http://www.pwc.com/us/en/
health-industries/publications/old-data-learns-new-tricks.jhtml](http://www.pwc.com/us/en/health-industries/publications/old-data-learns-new-tricks.jhtml) (last visited
August 12, 2014).

1 28. The three principal credit bureaus – Experian, Equifax and TransUnion –
2 produce very different reports, so the use of only one credit bureau monitoring service is an
3 inefficient monitoring strategy. Additionally, after affected Class Members sign up for a
4 program and provide the credit bureau with their contact information, the credit bureau,
5 seizing a golden opportunity to push other products and services, will solicit them with
6 advertising to purchase other products and services Sony decided not to provide or a
7 continuation of the short program it did offer. These advertisements exploit consumers who
8 are not fully informed of their rights, for example, to receive a free 90-day fraud alert on their
9 credit reports and obtain their credit reports from all three credit bureaus absolutely free.

10 **C. Sony Has a Long History of Data Breaches. Sony Knew Its Internal Computer**
11 **Systems and Networks Were Not Secure. Sony’s Cavalier Attitude Regarding the**
12 **Protection of Its Current and Former Employees’ and Independent Contractors’**
13 **PII/PHI Directly and Proximately Caused the Data Breach.**

14 29. Since 2005, Sony has experienced multiple data security failures in its internal
15 computer systems and networks.

16 30. Sony’s first foray into the world of data breaches was the infamous 2005 Sony
17 BMG copy protection rootkit scandal – where Sony BMG, Sony's music division, took an
18 aggressive position regarding digital rights management and incorporated two pieces of
19 malicious copy protection software in its CDs. The malicious software programs were
20 actually rootkits that modified a computer's operating system so the CDs could not be copied.

21 31. But the malicious software programs did not stop there. One of the programs
22 sent private data about its customers’ listening habits back to Sony servers, and the other
23 ironically took advantage of open source software in an apparent copyright violation. The
24 software would run constantly in the background, all the while sucking up computer resources.
25 There was no easy way to uninstall the programs – even if a customer knew about them. Even
26 worse, the rootkits made computers more vulnerable to cyberattacks. Over a period of two
27 years, Sony BMG sold over 21 million CDs containing the malicious software programs.

28 32. The ensuing scandal was huge, attracting attention from the Bush
Administration. The FTC also got involved. Several lawsuits were filed accusing Sony of

1 trading in malicious software and violating users' rights – which Sony settled. Meanwhile, the
2 debacle angered the hacker community. The rootkit scandal is arguably the Big Bang moment
3 for Sony's cybersecurity troubles – because when hackers become angry, they tend to hold a
4 grudge.

5 33. In December 2009, George Hotz, a 17-year-old high school student who
6 already had gained notoriety as the first person to carrier-unlock an iPhone, publicly
7 announced in advance that he was going to jailbreak the Sony PlayStation 3. This would allow
8 him to do various things, such as run pirated versions of games. Sony did nothing in response
9 to the announcement. Within two months, he completed the PlayStation 3 jailbreak, and
10 released the code to the public.

11 34. In an inadequate attempt to close the barn door after the horse got out, Sony
12 released a firmware update to patch the exploit, though other hackers followed Hotz's lead and
13 were ultimately able to run any software, including Linux, on a PlayStation 3.⁵ In January
14 2011, Hotz released the console's root keys for further hacking opportunities.

15 35. Thereafter, Sony sued Hotz and a number of other hackers, accusing them of
16 multiple counts of computer fraud and copyright infringement. Sony even convinced the
17 judge to unmask the IP addresses of the people who visited Hotz's website. Sony and Hotz
18 settled out of court in April 2011, when Hotz agreed not to hack into more Sony products.
19 Then Sony's real problems began.

20 36. As Sony was threatening to send George Hotz to jail, in early April 2011, the
21 hacker group known as “Anonymous” mobilized in a massive way, warning Sony that it had
22 launched a campaign to bring down the Sony PlayStation Network. Again, Sony did nothing.

23 37. Within two weeks of its warning, Anonymous took down the PlayStation
24 Network. The Network stayed down for twenty-three days, during which Anonymous also
25 obtained the PII of 77 million PlayStation account holders. The attack ended up costing Sony
26

27
28 ⁵ The Sony PlayStation 3 was originally lauded for its ability to run Linux, but Sony removed its Linux capability after another hack in 2010.

1 at least \$171 million. The hackers had sent a very clear message. Then, the floodgates
2 opened.

3 38. Following the Anonymous attack, Sony was attacked relentlessly. By one
4 security firm's count, there were twenty-one major incidents in the six months following the
5 initial PlayStation Network outage. Some of the attacks were relatively harmless breaches of
6 Sony's unprotected international websites, principally targeting Sony BMG and other music-
7 related businesses. Some the websites were defaced. Some were taken offline completely.
8 Some data was compromised.

9 39. But some of the system breaches following the devastating Sony PlayStation
10 Network breach were historically devastating in their own right. For example, in June 2011,
11 LulzSec broke into Sony Pictures' unprotected servers and secured private information,
12 including passwords and home addresses, of over 1,000,000 accounts. The hackers boasted on
13 the Internet that the data was easy to find and unencrypted. Passwords were just sitting there
14 in plain text – much like in this case where Sony openly stored thousands of passwords in a
15 folder named “Password.” Again, Sony did nothing.

16 40. The attacks kept coming. By the end of the six-month string of hacks, Sony's
17 stock price had fallen by nearly 40 percent. Although some data security experts thought the
18 attacks were an inside job since Sony fired a slew of people from the department that is
19 supposed to guard the company from cyberattacks, it seems more likely that these people were
20 just bad at their jobs.

21 41. For example, after the unprotected computer systems of a Sony division in one
22 country would be breached, Sony would not change a thing to protect the rest of its interests,
23 and then a week later, hackers would breach the unprotected computer systems of another
24 Sony division in another country in the exact same manner. It is even more astonishing that
25 Sony still had not secured its internal computer systems and network, and suffered the recent
26 company-wide Data Breach giving rise to this action. But that is exactly what happened – the
27 Guardians of Peace have proven that Sony left its entire network unprotected and vulnerable to
28

1 a single – albeit massive – data breach that released and disclosed Plaintiffs’ and Class
2 Members’ PII/PHI.

3 42. In February 2014, Jason Spaltro (“Spaltro”), then the Executive Director of
4 Information Security at SPE, notified Sony Chief Financial Officer David Hendler that a
5 significant amount of payment card information pertaining to 759 individuals in Brazil had
6 been obtained by fraudsters from Sony’s internal computer systems and network. The
7 compromised payment card information had been stored as .txt text files in a manner in which
8 Sony had stored this type of information since 2008. Spaltro, however, brushed off the
9 significance of the February 2014 data breach, and recommended against notifying the victims
10 that it had occurred.

11 43. In August 2014, a month after Sony settled the PlayStation class action
12 litigation resulting from the April 2011 data breach, hackers again took down the unprotected
13 PlayStation Network and Sony’s Entertainment Network by overwhelming the networks with
14 “denial of service” attacks. Also in August 2014, ARS Technica, an online information
15 technology publication, reported that, upon resigning as Sony’s Chief Information Security
16 Officer, Phil Reitingger remarked that there are a number of archaic systems that had been in
17 place at Sony for ages with plenty of potential attack points.

18 44. Attacks on Sony’s unprotected internal computer systems and networks have
19 continued – most recently on December 25, 2014, when hackers again took down the Sony
20 PlayStation Network for about three days.

21 45. The core of Sony’s problem is that its cybersecurity is totally inadequate. The
22 situation is further exacerbated by its corporate culture and flippant attitude towards protecting
23 its current and former employees’ and independent contractors’ PII/PHI. Indeed, Spaltro made
24 a business decision in November 2005 not to ensure the security of Sony’s internal computer
25 systems and network, even though he was warned by an auditor who had just completed a
26 review of Sony’s cybersecurity practices that Sony had several security weaknesses, including
27 insufficiently strong access controls, which is a key Sarbanes-Oxley requirement. Spaltro
28 subsequently stated in a 2007 interview with the business website CIO that he was not willing

1 to put up a lot of money to safeguard and protect Sony's sensitive information because "[i]t's a
2 valid business decision to accept the risk." CIO subsequently reported that Ari Schwartz, a
3 privacy expert with the Center for Democracy and Technology, believed Spaltro's reasoning to
4 be "shortsighted" because the cost of notification is only a small portion of the potential cost
5 of a data breach. Spaltro's business decision continues to haunt Sony to this day.

6 46. Sony's systemic and systematic pattern of internal computer systems and
7 network security failures and data breaches confirm its knowing inability, unwillingness,
8 failure, and refusal to correct its faulty data protection policies. Sony knew its data security
9 processes, controls, policies, procedures, protocols, and software and hardware systems were
10 insufficient, antiquated, inadequate, and did not safeguard and protect its current and former
11 employees' and independent contractors' PII/PHI, yet did nothing to expand, improve or
12 update them. On information and belief, Sony's pattern of willful and intentional disregard of
13 the security of its current and former employees' and independent contractors' PII/PHI in its
14 possession and control – which directly and proximately caused the Data Breach – continues
15 notwithstanding the repeated warnings it has received, the repeated data breaches it has
16 suffered, and the repeated embarrassment heaped upon it.

17 47. Sony's above-described wrongful actions, inaction, omissions, and want of
18 ordinary care, and the resulting Data Breach, demonstrate its intentional and reckless disregard
19 for Plaintiffs' and Class Members' protected privacy rights.

20 **D. The Sony Data Breach Was Preventable and Never Should Have Happened**

21 48. The Data Breach was preventable and never should have happened. Sony knew
22 (or should have known) its data security processes, controls, policies, procedures, protocols,
23 and software and hardware systems were insufficient, antiquated, inadequate, and did not
24 safeguard and protect its current and former employees' and independent contractors' PII/PHI,
25 yet did nothing to expand, improve, or update them.

26 49. The Data Breach could have been prevented had Sony properly addressed its
27 organizational issues after the 2011 PlayStation Network breach. Sony admittedly operated as
28 a collection of silos. Sony should have immediately instituted a cybersecurity sharing and

1 collaboration solution between their divisions and their supply chain. From 2011 forward,
2 Sony should have implemented standardized corporate-wide cybersecurity and beefed up
3 employee information security training across the organization. The tools and techniques
4 Sony decided to use to protect the unprotected PlayStation Network were a reactive approach –
5 Sony was attacked at point X by Y, so it defended point X with tools to stop successful
6 exploitation by those kinds of Y attacks. It was completely reactive, but not proactive. More
7 importantly, it did not work. *See* December 25, 2014 PlayStation Network breach (above).

8 50. The Data Breach also could have been prevented had Sony utilized the proper
9 data security processes, controls, policies, procedures, protocols, and software and hardware
10 systems. The email correspondence leaked in the Data Breach showed that Sony was
11 operating without (i) adequate protection against phishing attacks and remote-access Trojans,
12 (ii) password management policies, (iii) encrypting the PII/PHI, and (iv) data storage and
13 backups.

14 51. The Data Breach also could have been prevented had Sony used minimum
15 industry standards, such as adequate passwords. The password “password,” which was used
16 by Sony in three certificates, was used by the hackers to digitally sign the malware they
17 installed in Sony’s computer systems and networks. Sony also used weak passwords to protect
18 internal and Internet-facing critical servers within its computer systems and networks.

19 52. The Data Breach also could have been prevented had Sony conducted regular
20 and timely data security assessments. Sony failed to detect weak passwords and failed to
21 prevent the massive Data Breach. Most companies – such as Sony – treat the investment in
22 cybersecurity as an optional cost, and implement only what is required to be compliant. Sony
23 should have conducted penetration tests on a regular basis, using both automated pen-testing
24 tools and manual security checks. Sony, however, took the easy way out with its security
25 testing.

26 53. The Data Breach also could have been prevented had Sony installed the proper
27 computer system and network alarms, and properly monitored its systems and networks.
28 Numerous alarms should have been triggered while the computer systems and networks were

1 being breached and compromised. These notifications would have allowed Sony to
2 immediately identify the Data Breach, and mitigate the damages at an early stage. The
3 computer system and network alarms were either not in place, not taken seriously (possibly
4 due to many false alarms), or completely ignored. Actively monitoring logs, including event
5 logs, syslogs, web server logs, firewall logs, anti-virus logs and logging of the various
6 computer systems and networks running in the organization is tedious, but it would have saved
7 the day for Sony and allowed it to sound the alarm before it was too late. Various tools exist
8 that allow automation of log monitoring, including systems notifying the system administrator
9 when a data breach is detected. Here, Sony has been left to sift through the logs the hackers
10 left behind in order to identify the source and the real magnitude of the Data Breach.

11 54. The Data Breach also could have been prevented had Sony conducted
12 information security training throughout the company, explaining such concepts as complex
13 passwords and the reasons to use them, reporting anti-virus warnings as opposed to ignoring
14 them, recognizing attempts at social engineering, and avoiding connecting to work resources
15 from public WIFI networks.

16 55. The Data Breach could have been prevented had Sony instituted an effective
17 Enterprise Risk Management (“ERM”) system supported by the appropriate ERM software.
18 With an effective ERM process, the risk of a data breach would have been documented and
19 assessed in a way that would have provided transparency to Sony senior management who, in
20 turn, would have had the time and opportunity to take steps to prevent the Data Breach before
21 it occurred. Even for an entity the size of Sony, a fully developed ERM system would have
22 cost Sony substantially less than the estimated cost of the Data Breach.⁶ On information and
23 belief, however, Sony failed and refused to develop and implement an effective ERM system –
24 much less, an ERM system of any kind.

25
26 ⁶ According to the Ponemon Institute, a data breach costs U.S. companies an average of
27 \$201 for each compromised record containing sensitive and confidential PII/PHI – which pegs
28 the total estimated cost of the Data Breach to Sony in the billions of dollars. *See 2014 Cost of
Data Breach Study: United States*, PONEMON INSTITUTE (May 2014) at
<http://www.accudatasystems.com/assets/2014-cost-of-a-data-breach-study.pdf> (last visited
January 2, 2015).

1 56. The Data Breach also could have been prevented had Sony installed the
2 appropriate anti-virus software across all of its internal computer systems and networks.
3 Several readily available anti-virus software programs – such as AVG, Bitdefender and
4 ThreatTrack – would have detected and removed the malware used by the hackers. On
5 information and belief, however, Sony failed and refused to install the appropriate anti-virus
6 software across all of its internal computer systems and networks.

7 57. The key to effective data protection is layered security – which Sony did not
8 have in place. Had layered data security been in place, the fraudsters would have first had to
9 determine how to deploy the malware, and then determine how to circumvent the antivirus
10 software. Even if they could have accomplished these feats – which they would not have been
11 able to do – the malware would have been blocked by the firewall or network segmentation
12 when trying to access the Internet. Had Sony taken even the most fundamental layered data
13 security measures, the Data Breach would never have happened.

14 **E. The Sony Data Breach Inflicted (and Will Continue to Inflict) Economic Damages**
15 **and Other Injury and Actual Harm on Plaintiffs and Class Members**

16 58. Sony flagrantly disregarded and violated Plaintiffs' and Class Members'
17 privacy rights, and harmed them in the process, by not obtaining their prior written consent to
18 disclose their PII/PHI to any other person, entity, or government agency – as required by the
19 California CMIA, and other pertinent California laws, regulations, industry standards, and
20 internal company standards.

21 59. Sony flagrantly disregarded and violated Plaintiffs' and Class Members'
22 privacy rights, and harmed them in the process, by failing to safeguard and protect and, in fact,
23 wrongfully releasing, disclosing, and disseminating their PII/PHI to the world without
24 authorization.

25 60. Sony flagrantly disregarded and violated Plaintiffs' and Class Members'
26 privacy rights, and harmed them in the process, by failing to keep or maintain accurate records
27 of the precise PII/PHI wrongfully released, disclosed, and disseminated in the Data Breach.
28

1 61. Sony flagrantly disregarded and violated Plaintiffs' and Class Members'
2 privacy rights, and harmed them in the process, by failing to design, adopt, implement, control,
3 direct, oversee, manage, monitor and audit the appropriate data security processes, controls,
4 policies, procedures, protocols, and software and hardware systems to safeguard and protect
5 Plaintiff's and Class Members' PII/PHI. Sony's failure, refusal, and unwillingness – even in
6 the face of prior serious data breaches – is an abuse of discretion and confirms its intentional
7 and willful failure and refusal to observe procedures required by law, industry standards, and
8 its own internal policies and procedures.

9 62. Sony flagrantly disregarded and violated Plaintiffs' and Class Members'
10 privacy rights, and harmed them in the process, by failing to accurately and completely notify
11 and inform them about the Data Breach and corresponding loss of their PII/PHI.

12 63. Sony's inadequate Data Breach notification – including its failure to provide
13 Plaintiffs and Class Members with adequate and reasonable protection or sufficient relief from
14 the Data Breach – substantially increased their risk of identity theft, identity fraud or medical
15 fraud.

16 64. Identity theft occurs when a person's PII, such as their name, Social Security
17 number, driver license number, bank account information, credit card information, and account
18 usernames and passwords are used without their permission to commit fraud or other crimes.
19 *See* Federal Trade Commission, *Take Charge: Fighting Back Against Identity Theft* (February
20 2006), available at [http://www.businessidtheft.org/Portals/0/Docs/FTC%20-%20ID%20Theft](http://www.businessidtheft.org/Portals/0/Docs/FTC%20-%20ID%20Theft%20Guide.pdf)
21 [%20Guide.pdf](http://www.businessidtheft.org/Portals/0/Docs/FTC%20-%20ID%20Theft%20Guide.pdf) (last visited January 2, 2015).⁷

22 65. According to the FTC, the range of privacy-related harms is more expansive
23 than economic or physical harm or unwarranted intrusions and that any privacy framework
24

25
26 ⁷ According to the Federal Trade Commission ("FTC"), "Identity theft is a serious crime. People whose identities have been stolen can spend months or years – and thousands of dollars – cleaning up the mess the thieves have made of a good name and credit record. In the meantime, victims of identity theft may lose job opportunities, be refused loans for education, housing, or cars, and even get arrested for crimes they didn't commit. Humiliation, anger, and frustration are among the feelings victims experience as they navigate the process of rescuing their identity." *Id.*

1 should recognize additional harms that might arise from unanticipated uses of data.⁸ Further,
2 according to the FTC, there is significant evidence demonstrating that technological advances
3 and the ability to combine disparate pieces of data can lead to identification of a consumer,
4 computer or device even if the individual pieces of data do not constitute PII.⁹

5 66. According to Javelin Strategy & Research's 2012 Identity Fraud Report (the
6 "Javelin Report"), as recently as 2011, the mean consumer cost of rectifying identity fraud was
7 \$354 while the mean resolution time of identity fraud was 12 hours. *Id.* at 6. In 2011, the
8 consumer cost for new account fraud and existing non-card fraud increased 33% and 50%
9 respectively. *Id.* at 9. Consumers who received a data breach notification had a fraud
10 incidence rate of 19% in 2011 and, of those experiencing fraud, 43% reported their credit card
11 numbers were stolen and 22% of the victims reported their debit card numbers were stolen. *Id.*
12 at 10. More important, consumers who were notified that their PII/PHI had been breached
13 were 9.5 times more likely to experience identity fraud than consumers who did not receive
14 such a notification. *Id.* at 39.

15 67. Sony's inadequate Data Breach notification also increased Plaintiffs' and Class
16 Members' risk of "phishing" (as defined above).

17 68. When a fraudster has access to PII/PHI from a large group of similarly situated
18 victims – such as Plaintiff and Class Members – it is much more feasible to develop a
19 believable phishing spoof email that appears realistic. The fraudsters can then convince the
20 group of victims to reveal additional PII/PHI.

21 69. A person whose personal information has been compromised may not see any
22 signs of identity theft for *years*. According to the GAO's June 2007 report on Data Breaches:

23 [L]aw enforcement officials told us that in some cases, stolen data may be held
24 for up to a year or more before being used to commit identity theft. Further,
25 once stolen data have been sold or posted on the Web, fraudulent use of that
26 information may continue for years. As a result, studies that attempt to measure
the harm resulting from data breaches cannot necessarily rule out all future
harm.

27 ⁸ Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change:
28 A Proposed Framework for Businesses and Policymakers* (March 2012), available at
<http://www.ftc.gov/os/2012/03/120326privacyreport.pdf> (last visited January 2, 2015).

⁹ *Id.*

1 70. PII/PHI is such a valuable commodity to identity thieves that once the
2 information has been compromised, criminals often trade the information on the “cyber black-
3 market” for years. Identity thieves and other cyber criminals openly post credit card numbers,
4 Social Security numbers, medical files, and other PII/PHI directly on various Internet websites,
5 thereby making the information publicly available. In one study, researchers found hundreds
6 of websites displaying compromised PII/PHI. Strikingly, none of these websites were blocked
7 by Google’s safeguard filtering mechanism – the “Safe Browsing list.” The study concluded:

8 It is clear from the current state of the credit card black-market that cyber
9 criminals can operate much too easily on the Internet. They are not afraid to
10 put out their email addresses, in some cases phone numbers and other
11 credentials in their advertisements. It seems that the black market for cyber
12 criminals is not underground at all. In fact, it’s very “in your face.”¹⁰

12 71. “[H]ealth information is far more valuable than Social Security numbers” on
13 the cyber black market, according to Dr. Deborah Peel, founder and chairwoman of Patient
14 Privacy Rights.¹¹ An ABC News search uncovered one internet seller offering medical record
15 database dumps for \$14 to \$25 per person. *Id.* ABC News was then sent, unsolicited, 40
16 individuals’ private health information, including their names, addresses and body mass index.
17 *Id.* Another inquiry yielded an offer of more than 100 records, including everything from
18 Social Security numbers to persons suffering from anxiety, hypertension, and their HIV status.
19 Plaintiffs’ and Class Members’ PII/PHI could similarly be valued and traded on the cyber
20 black market. *Id.*

21 72. Sony flagrantly disregarded and violated Plaintiffs’ and Class Members’
22 privacy rights, and harmed them in the process, by depriving them of the value of their
23 PII/PHI, for which there is a well-established national and international market. *See, e.g.,*
24 *Soma, supra* (“PII, which companies obtain at little cost, has quantifiable value that is rapidly
25

26
27 ¹⁰ *See* <http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/> (last visited January 2, 2015).

28 ¹¹ *See* <http://abcnews.go.com/Health/medical-records-private-abc-news-investigation/story?id=17228986> (last visited January 2, 2015).

1 reaching a level comparable to the value of traditional financial assets.”) (citations omitted);
2 ABC News Report, *supra*.

3 73. Aside from the criminal element, frequent purchasers of purloined PHI include
4 pharmacies, drug manufacturers, medical device manufacturers, hospitals, and insurance
5 companies who use the information to market their products and services directly to data
6 breach victims and adjust the victims’ medical insurance premiums. *Id.* Plaintiffs and Class
7 Members, not data thieves, should have the right to sell their PII/PHI and receive the
8 corresponding financial benefits, and the right to decide to have their PII/PHI not sold either.

9 74. The actual harm and adverse effects to Plaintiffs and Class Members, including
10 the imminent, immediate and continuing increased risk of harm for identity theft, identity
11 fraud or medical fraud directly and proximately caused by Sony’s above-described wrongful
12 actions, inaction, omissions, and want of ordinary care, and the resulting Data Breach, requires
13 Plaintiffs and Class Members to take affirmative acts to recover their peace of mind, and
14 personal security – for which there is a financial and temporal cost. Plaintiffs and Class
15 Members have spent significant time and expense engaging in such actions, including, without
16 limitation, (i) identifying and dealing with fraudulent charges, (ii) canceling and securing the
17 reissuance of credit cards and debit cards, (iii) frequently purchasing credit reports from
18 multiple credit reporting agencies, (iv) placing and removing fraud alerts and security freezes
19 on credit reports, (v) purchasing credit monitoring and internet monitoring services, (vi)
20 purchasing identity theft insurance, (vii) reviewing bank statements, credit card statements,
21 and other financial account statements, (viii) closing, modifying and reopening bank accounts
22 and other financial accounts, (ix) dealing with withdrawal and purchase limits imposed on
23 compromised accounts, (x) experiencing the inability to withdraw funds from compromised
24 accounts, (xi) making trips to their financial institutions, (xii) spending time on the telephone
25 attempting to sort out issues related to the Data Breach, (xiii) resetting automatic billing
26 instructions tied to compromised accounts, (xiv) paying late fees and declined payment fees
27 imposed as a result of failed automatic payments, (xv) changing email addresses, or (xvi)
28 updating financial and non-financial accounts with new bank account information, new

1 payment card information, and new email addresses. Plaintiffs and Class Members have
2 suffered, and will continue to suffer, such damages for the foreseeable future.

3 75. Victims and potential victims of identity theft, identity fraud or medical fraud –
4 such as Plaintiffs and Class Members – typically spend hundreds of hours in personal time and
5 hundreds of dollars in personal funds to resolve credit and other financial issues resulting from
6 data breaches. According to the Javelin Report, not only is there a substantially increased risk
7 of identity theft and identity fraud for data breach victims, those who are further victimized by
8 identity theft or identity fraud will incur an average fraud-related economic loss of \$1,513 and
9 incur an average of \$354 of out-of-pocket expenses attempting to rectify the situation. *Id.* at 6.

10 76. Other statistical analyses are in accord. The GAO found that identity thieves
11 use PII/PHI to open financial accounts and payment card accounts and incur charges in a
12 victim's name. This type of identity theft is the "most damaging" because it may take some
13 time for the victim to become aware of the theft, in the meantime causing significant harm to
14 the victim's credit rating and finances. Moreover, unlike other PII/PHI, Social Security
15 numbers are incredibly difficult to change and their misuse can continue for years into the
16 future.

17 77. Identity thieves also use Social Security numbers to commit other types of
18 fraud, such as obtaining false identification cards, obtaining government benefits in the
19 victim's name, committing crimes, and filing fraudulent tax returns on the victim's behalf to
20 obtain fraudulent tax refunds. Identity thieves also obtain jobs using compromised Social
21 Security numbers, rent houses and apartments and obtain medical services in the victim's
22 name. Identity thieves also have been known to give a victim's personal information to police
23 during an arrest, resulting in the issuance of an arrest warrant in the victim's name and an
24 unwarranted criminal record. The GAO states that victims of identity theft face "substantial
25 costs and inconvenience repairing damage to their credit records," as well the damage to their
26 "good name."

27 78. The unauthorized disclosure of a person's Social Security number can be
28 particularly damaging since Social Security numbers cannot be easily replaced like a credit

1 card or debit card. In order to obtain a new Social Security number, a person must show
2 evidence that someone is using the number fraudulently or is being disadvantaged by the
3 misuse. *See Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064
4 (December 2013), available at <http://www.ssa.gov/pubs/10064.html> (last visited January 2,
5 2015). Thus, a person whose PII/PHI has been compromised cannot obtain a new Social
6 Security number until the damage has already been done.

7 79. Obtaining a new Social Security number also is not an absolute prevention
8 against identity theft. Government agencies, private businesses and credit reporting companies
9 likely maintain a victim's records under the old number, so using a new Social Security
10 number will not guarantee a fresh start. For some identity theft and identity fraud victims, a
11 new number may create new problems. Because prior positive credit information is not
12 associated with the new Social Security number, it is more difficult to obtain credit due to the
13 absence of a credit history.

14 80. Medical identity theft (or medical fraud) occurs when a person's personal
15 information is used without authorization to obtain, or receive payment for, medical treatment,
16 services or goods. For example, according to the most recent census, as of 2010, more than 50
17 million people in the United States did not have health insurance. This in turn has led to a
18 surge in medical identity theft as a means of fraudulently obtaining medical care. Victims of
19 medical identity theft also may find that their medical records are inaccurate, which can have a
20 serious impact on their ability to obtain proper medical care and insurance benefits.

21 81. Sony's above-described wrongful actions, inaction, omissions, and want of
22 ordinary care directly and proximately caused the "double Holy Grail of data breaches" – the
23 release, disclosure, and dissemination into the public domain of Plaintiffs' and Class
24 Members' PII/PHI without their knowledge, authorization or consent. As a direct and
25 proximate result of Sony's above-described wrongful actions, inaction, omissions, and want of
26 ordinary care, and the resulting Data Breach, Plaintiffs and Class Members have incurred (and
27 will continue to incur) economic damages and other injury and harm in the form of, *inter alia*,
28 (i) actual identity theft, identity fraud or medical fraud, (ii) invasion of privacy, (iii) breach of

1 the confidentiality of their PII/PHI, (iv) statutory nominal damages of \$1000 per Plaintiff and
2 each Class Member under the CMIA (CAL. CIV. CODE § 56.36(b)(1)), (v) expenses and losses
3 in discharging their duties (CAL. LAB. CODE §§ 2800 and 2802), (vi) deprivation of the value
4 of their PII/PHI, for which there is a well-established national and international market, (vii)
5 the financial and temporal cost of monitoring their credit, monitoring their financial accounts,
6 and mitigating their damages (*see above*), and (viii) the imminent, immediate and continuing
7 increased risk of identity theft, identity fraud or medical fraud – for which they are entitled to
8 compensation.

9 **CLASS ACTION ALLEGATIONS**

10 82. Pursuant to CAL. CIV. PROC. § 382, Plaintiffs bring this action against Sony as a
11 class action on behalf of themselves and all members of the following class of similarly
12 situated persons:

13 All current and former Sony employees and independent contractors in
14 California whose names, addresses, Social Security numbers, medical histories,
15 employment records, human resources records, or financial information
16 (PII/PHI) was maintained on a Sony computer system server that was breached
17 on or about November 24, 2014, and released and disclosed without
18 authorization.

19 83. Plaintiffs also seek to represent sub-classes composed of and defined as
20 follows:

21 (A) All current and former Sony employees in California whose names,
22 addresses, Social Security numbers, medical histories, employment records,
23 human resources records, or financial information (PII/PHI) was maintained on
24 a Sony computer system server that was breached on or about November 24,
25 2014, and released and disclosed without authorization (“Sony Employee Sub-
26 Class”); and

27 (B) All current and former Sony independent contractors in California
28 whose names, addresses, Social Security numbers, medical histories,
employment records, human resources records, or financial information
(PII/PHI) was maintained on a Sony computer system server that was breached
on or about November 24, 2014, and released and disclosed without
authorization (“Sony Independent Contractor Sub-Class”).

1 84. Plaintiffs reserve the right under Rule 1855(b) of the California Rules of Court
2 to amend or modify the Class description with greater specificity or further division into
3 subclasses or limitation to particular issues.

4 85. Excluded from the Class and Sub-Classes are Sony, any entity in which Sony or
5 any Sony subsidiary has a controlling interest, Sony's officers, directors, agents and legal
6 representatives, and the Court and Court personnel.

7 86. The Class Members are so numerous that their joinder is impracticable.
8 According to information disclosed by Sony in the media, there are over 47,000 Class
9 Members. The precise number, identity, and contact information of each Class Member is
10 currently unknown to Plaintiffs, but can be easily derived from the internal records Sony used
11 to send the Data Breach Notification Letters to Plaintiffs and Class Members.

12 87. The rights of Plaintiffs and each Class Member were violated in a virtually
13 identical manner as a direct and proximate result of Sony's wrongful actions, inaction,
14 omissions, and want of ordinary care that, in turn, directly and proximately caused the Data
15 Breach and the unauthorized release and disclosure of their PII/PHI.

16 88. There are questions of law and fact common to the Class as a whole that
17 predominate over any questions affecting only individual members of the Class including,
18 without limitation:

- 19 (i) Whether Sony adequately designed, adopted, implemented, controlled, directed,
20 oversaw, managed, monitored and audited the appropriate data security
21 processes, controls, policies, procedures, protocols, and software and hardware
22 systems to safeguard and protect Plaintiffs' and Class Members' PII/PHI that
23 was disclosed without authorization in the Data Breach;
- 24 (ii) Whether Sony's failure to properly safeguard and protect Plaintiffs' and Class
25 Members' PII/PHI was willful, reckless, arbitrary, capricious and otherwise not
26 in accordance with applicable protocols, procedures, guidelines, laws and
27 regulations;
- 28 (iii) Whether Sony failed to inform Plaintiffs and Class Members of the Data
Breach and the unauthorized disclosure of their PII/PHI in a manner, and within
the time period, required by its own internal policies and procedures and the
applicable laws;
- (iv) Whether Sony's wrongful actions, inaction, omissions, and want of ordinary
care that directly and proximately caused the Data Breach and the unauthorized

- 1 disclosure of Plaintiffs' and Class Members' PII/PHI violated the California
2 CMIA (CAL. CIV. CODE § 56, *et seq.*);
- 3 (v) Whether Sony's wrongful actions, inaction, omissions, and want of ordinary
4 care that directly and proximately caused the Data Breach and the unauthorized
5 disclosure of Plaintiffs' and Class Members' PII/PHI violated the California
6 Unfair Competition Law (CAL. BUS. & PROF. CODE § 17200, *et seq.*);
- 7 (vi) Whether Sony's wrongful actions, inaction, omissions, and want of ordinary
8 care that directly and proximately caused the Data Breach and the unauthorized
9 disclosure of Plaintiffs' and Class Members' PII/PHI violated the California
10 Security Requirements for Consumer Records (CAL. CIV. CODE §§ 1798.29 and
11 1798.80, *et seq.*);
- 12 (vii) Whether Sony's wrongful actions, inaction, omissions, and want of ordinary
13 care that directly and proximately caused the Data Breach and the unauthorized
14 disclosure of Plaintiffs' and Class Members' PII/PHI constitutes negligence at
15 California common law;
- 16 (viii) Whether Sony's wrongful actions, inaction, omissions, and want of ordinary
17 care that directly and proximately caused the Data Breach and the unauthorized
18 disclosure of Plaintiffs' and Class Members' PII/PHI constitutes invasion of
19 privacy by public disclosure of private facts at California common law;
- 20 (ix) Whether Sony's wrongful actions, inaction, omissions, and want of ordinary
21 care that directly and proximately caused the Data Breach and the unauthorized
22 disclosure of Plaintiffs' and Class Members' PII/PHI constitutes unjust
23 enrichment/assumpsit at California common law;
- 24 (x) Whether Plaintiffs and Class Members suffered harm or injury as a direct and
25 proximate result of Sony's wrongful actions, inaction, omissions, and want of
26 ordinary care that directly and proximately caused the Data Breach and the
27 unauthorized disclosure of Plaintiffs' and Class Members' PII/PHI;
- 28 (xi) Whether Plaintiffs and Class Members suffered damages as a direct and
proximate result of Sony's wrongful actions, inaction, omissions, and want of
ordinary care that directly and proximately caused the Data Breach and the
unauthorized disclosure of Plaintiffs' and Class Members' PII/PHI and, if so,
the amount of such damages;
- (xii) Whether Plaintiffs and Sony Employee Sub-Class Members are entitled to
indemnification under CAL. LABOR CODE §§ 2800 and 2802 as a direct and
proximate result of Sony's wrongful actions, inaction, omissions, and want of
ordinary care that directly and proximately caused the Data Breach and the
unauthorized disclosure of Plaintiffs' and Class Members' PII/PHI; and
- (xiii) Whether Plaintiffs and Class Members are entitled to statutory and punitive
damages as a direct and proximate result of Sony's wrongful actions, inaction,
omissions, and want of ordinary care that directly and proximately caused the
Data Breach and the unauthorized disclosure of Plaintiffs' and Class Members'
PII/PHI.

1 89. Plaintiffs' claims are typical of the claims of the Class Members because
2 Plaintiffs, like all Class Members, are victims of Sony's wrongful actions, inaction, and
3 omissions, and want of ordinary care that directly and proximately caused the Data Breach,
4 caused the unauthorized disclosure of Plaintiffs' and Class Members' PII/PHI, and caused
5 Plaintiffs and Class Members to suffer the resulting economic damages, injury and harm.

6 90. Plaintiffs and their counsel will fairly and adequately represent the interests of
7 the Class Members. Plaintiffs have no interests antagonistic to, or in conflict with, any of the
8 Class Members' interests. Plaintiffs' lawyers are highly experienced in the prosecution of
9 complex commercial litigation, employment litigation, and data breach class actions.

10 91. A class action is superior to all other available methods for fairly and efficiently
11 adjudicating Plaintiffs' and Class Members' claims. Plaintiffs and Class Members have been
12 irreparably harmed as a direct and proximate result of Sony's wrongful actions, inaction,
13 omissions, and want of ordinary care that caused the Data Breach and the unauthorized
14 disclosure of Plaintiffs' and Class Members' PII/PHI. Litigating this case as a class action is
15 appropriate because (i) it will avoid a multiplicity of suits and the corresponding burden on the
16 courts and Parties, (ii) it would be virtually impossible for all Class Members to intervene as
17 parties-plaintiff in this action, (iii) it will allow numerous individuals with claims too small to
18 adjudicate on an individual basis because of prohibitive litigation costs to obtain redress for
19 their injuries, and (iv) it will provide court oversight of the claims process once Sony's
20 liability is adjudicated.

21 92. Certification of the Class, therefore, is appropriate because the above-described
22 common questions of law or fact predominate over any questions affecting individual Class
23 Members, and a class action is superior to other available methods for the fair and efficient
24 adjudication of this controversy.

25 93. Certification of the Class also is appropriate because Sony has acted, or refused
26 to act, on grounds generally applicable to the Class, thereby making appropriate final
27 injunctive relief and equitable relief with respect to the Class as a whole.

28

1 94. Certification of the Class also is appropriate because the prosecution of separate
 2 actions by individual Class Members would create a risk of establishing incompatible
 3 standards of conduct for Sony. For example, one court might decide the challenged wrongful
 4 actions, inaction, omissions, and want of ordinary care are illegal and enjoin Sony, while
 5 another court might decide that the same wrongful actions, inaction, omissions, and want of
 6 ordinary care are not illegal. Individual actions also could be dispositive of the interests of the
 7 other Class Members who were not parties to such actions and substantially impair or impede
 8 their ability to protect their interests.

9 95. Sony's wrongful actions, inaction, omissions, and want of ordinary care that
 10 directly and proximately caused the Data Breach are generally applicable to the Class as a
 11 whole, and Plaintiffs seek, *inter alia*, equitable remedies with respect to the Class as a whole.

12 96. Sony's systemic policies and practices also make injunctive relief with respect
 13 to the Class as a whole appropriate.

14 97. Absent a class action, Sony will retain the benefits of its wrongdoing despite its
 15 serious violations of the law and infliction of economic damages, injury and actual harm on
 16 Plaintiffs and Class Members.

CLAIMS AND CAUSES OF ACTION

COUNT I

VIOLATION OF THE CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT (CAL. CIV. CODE § 56, *et seq.*)

(On Behalf of Plaintiffs and Each Class Member)

22 98. The preceding factual statements and allegations are incorporated by reference.

23 99. Section 56.10(a) of the California Civil Code provides that “[a] provider of
 24 health care, health care service plan, or contractor shall not disclose medical information
 25 regarding a patient of the provider of health care or an enrollee or subscriber of a health care
 26 plan without first obtaining an authorization.”

27 100. At all relevant times, Sony was both a contractor and a health care provider
 28 because it had the “purpose of maintaining medical information . . . in order to make the

1 information available to an individual or to a provider of health care at the request of the
2 individual or a provider of health care, for purposes of allowing the individual to manage his
3 or her information, or for the diagnosis or treatment of the individual.” CAL. CIV. CODE §
4 56.06(a).

5 101. At all relevant times, Sony collected, stored, managed, and transmitted
6 Plaintiffs’ and Class Members’ PII/PHI.

7 102. The CMIA requires Sony to implement and maintain standards of
8 confidentiality with respect to all individually identifiable PHI disclosed to it, and maintained
9 by it. Specifically, CAL. CIV. CODE § 56.10(a) prohibits Sony from disclosing Plaintiffs’ and
10 Class Members’ PHI without first obtaining their authorization to do so.

11 103. Section 56.11 of the California Civil Code specifies the manner in which
12 authorization must be obtained before PHI is released. Sony, however, failed to obtain the
13 proper authorization – much less, any authorization – from Plaintiffs and Class Members
14 before releasing and disclosing their PHI. Sony also failed to identify, implement, maintain
15 and monitor the proper data security measures, policies, procedures, protocols, and software
16 and hardware systems to safeguard and protect Plaintiffs’ and Class Members’ PHI as required
17 by California law. As a direct and proximate result of Sony’s wrongful actions, inaction,
18 omissions, and want of ordinary care, Plaintiffs’ and Class Members’ PHI was wrongfully
19 disseminated to the world. By disclosing Plaintiffs’ and Class Members’ PHI without their
20 written authorization, Sony violated California Civil Code § 56, *et seq.*, and its legal duty to
21 protect the confidentiality of such information.

22 104. Sony also violated Sections 56.06 and 56.101 of the California CMIA, which
23 prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction
24 or disposal of confidential PHI. As a direct and proximate result of Sony’s wrongful actions,
25 inaction, omissions, and want of ordinary care that directly and proximately caused the Data
26 Breach, Plaintiffs’ and Class Members’ confidential PHI was wrongfully released and
27 disclosed without their authorization.

28

1 ordinary care that directly and proximately caused the Data Breach, Sony engaged in unlawful,
2 unfair and fraudulent practices within the meaning, and in violation of, the UCL.

3 109. In the course of conducting its business, Sony committed “unlawful” business
4 practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee,
5 manage, monitor and audit appropriate data security processes, controls, policies, procedures,
6 protocols, and software and hardware systems to safeguard and protect Plaintiffs’ and Class
7 Members’ PII/PHI – even after suffering at least one recent widespread corporate data breach
8 – violating the statutory and common law alleged herein in the process, including, *inter alia*,
9 the California CMIA, the California Security Requirements for Consumer Records Act, and
10 Cal. Lab. Code §§ 2698, 2800 and 2802. Plaintiffs and Class Members reserve the right to
11 allege other violations of law by Sony constituting other unlawful business acts or practices.
12 Sony’s above-described wrongful actions, inaction, omissions, and want of ordinary care are
13 ongoing and continue to this date.

14 110. Sony also violated the UCL by failing to timely notify Plaintiffs and Class
15 Members regarding the unauthorized release and disclosure of their PII/PHI. If Plaintiffs and
16 Class Members had been notified in an appropriate fashion, they could have taken precautions
17 to safeguard and protect their PII/PHI, finances, medical information, and identities.

18 111. Sony’s above-described wrongful actions, inaction, omissions, want of ordinary
19 care, misrepresentations, practices, and non-disclosures also constitute “unfair” business acts
20 and practices in violation of the UCL in that Sony’s wrongful conduct is substantially injurious
21 to consumers, offends public policy, and is immoral, unethical, oppressive, and unscrupulous.
22 The gravity of Sony’s wrongful conduct outweighs any alleged benefits attributable to such
23 conduct. There were reasonably available alternatives to further Sony’s legitimate business
24 interests other than engaging in the above-described wrongful conduct.

25 112. The UCL also prohibits any “fraudulent business act or practice.” Sony’s
26 above-described claims, nondisclosures and misleading statements were false, misleading and
27 likely to deceive the consuming public in violation of the UCL.
28

1 113. As a direct and proximate result of Sony's above-described wrongful actions,
2 inaction, omissions, and want of ordinary care that directly and proximately caused the Data
3 Breach and its violations of the UCL, Plaintiffs and Class Members have suffered (and will
4 continue to suffer) economic damages and other injury and actual harm in the form of, *inter*
5 *alia*, (i) actual identity theft, identity fraud or medical fraud, (ii) invasion of privacy, (iii)
6 breach of the confidentiality of their PII/PHI, (iv) statutory nominal damages of \$1000 per
7 Plaintiff and each Class Member under the CMIA (CAL. CIV. CODE §56.36(b)(1)), (v)
8 expenses and losses in discharging their duties (CAL. LAB. CODE §§ 2800 and 2802), (vi)
9 deprivation of the value of their PII/PHI, for which there is a well-established national and
10 international market, (vii) the financial and temporal cost of monitoring their credit,
11 monitoring their financial accounts, and mitigating their damages (*see* above), and (viii) the
12 imminent, immediate and continuing increased risk of identity theft, identity fraud or medical
13 fraud – for which they are entitled to compensation.

14 114. As part of its corporate culture, Sony has taken – and touted – a cavalier
15 attitude towards safeguarding and protecting PII/PHI in its possession, custody, and control
16 and a cavalier attitude towards cyber security. As a result, Sony has released and disclosed
17 sensitive and confidential PII and PHI entrusted to it on multiple prior occasions. Unless
18 restrained and enjoined, Sony will continue to engage in the above-described wrongful
19 conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of themselves,
20 Class Members, and the general public, also seek restitution and an injunction prohibiting
21 Sony from continuing such wrongful conduct, and requiring Sony to modify its corporate
22 culture and design, adopt, implement, control, direct, oversee, manage, monitor and audit
23 appropriate data security processes, controls, policies, procedures protocols, and software and
24 hardware systems to safeguard and protect the PII/PHI entrusted to it, as well as all other relief
25 the Court deems appropriate, consistent with CAL. BUS. & PROF. CODE § 17203.

26 ///

27 ///

28 ///

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

COUNT III

VIOLATION OF SECURITY REQUIREMENTS FOR CONSUMER RECORDS

(CAL. CIV. CODE §§ 1798.29 and 1798.80, et seq.)

(On Behalf of Plaintiffs and Each Class Member)

115. The preceding factual statements and allegations are incorporated by reference.

116. California law requires any business that obtains, possesses and controls PII/PHI to implement and maintain reasonable security procedures and practices to protect such information from unauthorized access, destruction, use, modification or disclosure.

117. Under CAL. CIV. CODE §§ 1798.29 and 1798.82, any business that obtains and retains PII/PHI must promptly and “in the most expedient time possible and without unreasonable delay” disclose any Data Breach involving such retained data.

118. By its above-described wrongful actions, inaction, omissions, and want of ordinary care, Sony failed to and design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs’ and Class Members’ PII/PHI.

119. Sony also unreasonably delayed and failed to disclose the Data Breach to Plaintiffs and Class Members in the most expedient time possible and without unreasonable delay when it knew, or reasonably believed, Plaintiffs’ and Class Members’ PII/PHI had been wrongfully disclosed to an unauthorized person or persons and disseminated to the world by its posting on the Internet.

120. On information and belief, no law enforcement agency determined or instructed Sony that notifying Plaintiffs and Class Members about the Data Breach would impede a criminal investigation.

121. Sony also failed to comply with the privacy notification rights required by CAL. CIV. CODE § 1798.83.

122. As a direct and proximate result of Sony’s above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data

1 Breach and its violations of CAL. CIV. CODE §§ 1798.29 and 1798.82, Plaintiffs and Class
2 Members have suffered (and will continue to suffer) economic damages and other injury and
3 actual harm in the form of, *inter alia*, (i) actual identity theft, identity fraud or medical fraud,
4 (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory
5 nominal damages of \$1000 per Plaintiff and each Class Member under the CMIA (CAL. CIV.
6 CODE § 56.36(b)(1)), (v) expenses and losses in discharging their duties (CAL. LAB. CODE §§
7 2800 and 2802), (vi) deprivation of the value of their PII/PHI, for which there is a well-
8 established national and international market, (vii) the financial and temporal cost of
9 monitoring their credit, monitoring their financial accounts, and mitigating their damages (*see*
10 above), and (viii) the imminent, immediate and continuing increased risk of identity theft,
11 identity fraud or medical fraud – for which they are entitled to compensation.

12 COUNT IV

13 INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS

14 (On Behalf of Plaintiffs and Each Class Member)

15 123. The preceding factual statements and allegations are incorporated by reference.

16 124. Sony's intentional failure to safeguard and protect Plaintiffs' and Class
17 Members' PII/PHI directly and proximately resulted in the invasion of their privacy by the
18 public release and disclosure of such highly confidential and private information without
19 authorization.

20 125. Access to Plaintiffs' and Class Members' PII/PHI, and the wrongful
21 dissemination of such information into the public domain via publication on the Internet, was
22 easily achieved because the PII/PHI was either encrypted improperly or not encrypted at all.

23 126. Sony's wrongful release, disclosure, and dissemination of Plaintiffs' and Class
24 Members' PII/PHI into the public domain is of a legitimate public concern; publicity of their
25 PII/PHI would be, is and will continue to be offensive to reasonable people.

26 127. Sony intentionally invaded Plaintiffs' and Class Members' privacy by
27 repeatedly failing and refusing to design, adopt, implement, control, direct, oversee, manage,
28 monitor and audit appropriate data security processes, controls, policies, procedures, protocols,

1 and software and hardware systems to safeguard and protect Plaintiffs' and Class Members'
2 PII/PHI.

3 128. Sony's above-described wrongful actions, inaction, omissions, and want of
4 ordinary care that directly and proximately caused the Data Breach constituted (and continue
5 to constitute) an invasion of Plaintiffs' and Class Members' privacy by publicly disclosing
6 their private facts (*i.e.*, their PII/PHI) at California common law.

7 129. As a direct and proximate result of Sony's above-described wrongful actions,
8 inaction, omissions, and want of ordinary care that directly and proximately caused the Data
9 Breach, Plaintiffs and Class Members have suffered (and will continue to suffer) economic
10 damages and other injury and actual harm in the form of, *inter alia*, (i) actual identity theft,
11 identity fraud or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of
12 their PII/PHI, (iv) statutory nominal damages of \$1000 per Plaintiff and each Class Member
13 under the CMIA (CAL. CIV. CODE § 56.36(b)(1)), (v) expenses and losses in discharging their
14 duties (CAL. LAB. CODE §§ 2800 and 2802), (vi) deprivation of the value of their PII/PHI, for
15 which there is a well-established national and international market, (vii) the financial and
16 temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating
17 their damages (*see* above), and (viii) the imminent, immediate and continuing increased risk of
18 identity theft, identity fraud or medical fraud – for which they are entitled to compensation.

19 **COUNT V**

20 **NEGLIGENCE/GROSS NEGLIGENCE/NEGLIGENCE PER SE**

21 **(On Behalf of Plaintiffs and Each Class Member)**

22 130. The preceding factual statements and allegations are incorporated by reference.

23 131. Sony had (and continues to have) a duty to Plaintiffs and Class Members to
24 exercise reasonable care in safeguarding and protecting their PII/PHI.

25 132. Sony also had (and continues to have) a duty to use ordinary care in activities
26 from which harm might be reasonably anticipated (such as in the storage and protection of
27 private, non-public PII/PHI within its possession, custody and control). Such affirmative
28 duties also are expressly imposed upon Sony from other sources enumerated herein.

1 133. Sony also had (and continues to have) a duty to establish and foster a corporate
2 culture that supports safeguarding and protecting PII/PHI within its possession, custody and
3 control, and design, adopt, implement, control, direct, oversee, manage, monitor and audit
4 appropriate data security processes, controls, policies, procedures protocols, and software and
5 hardware systems to safeguard and protect the PII/PHI entrusted to it – including Plaintiffs’
6 and Class Members’ PII/PHI.

7 134. Sony’s duties arise from, *inter alia*, CAL. CIV. CODE § 56, *et seq.*, CAL. BUS. &
8 PROF. CODE § 17200, *et seq.*, and CAL. CIV. CODE § 1798.29; 1798.80, *et seq.*

9 135. The above-outlined standards and duties exist for the express purpose of
10 protecting Plaintiffs, Class Members and their PII/PHI.

11 136. Sony violated these standards and duties by failing to exercise reasonable care
12 in safeguarding and protecting Plaintiffs’ and Class Members’ PII/PHI by failing to design,
13 adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data
14 security processes, controls, policies, procedures, protocols, and software and hardware
15 systems to safeguard and protect PII/PHI entrusted to it – including Plaintiffs’ and Class
16 Members’ PII/PHI.

17 137. It was reasonably foreseeable to Sony that its failure to exercise reasonable care
18 in safeguarding and protecting Plaintiffs’ and Class Members’ PII/PHI by failing to design,
19 adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data
20 security processes, controls, policies, procedures, protocols, and software and hardware
21 systems would result in the unauthorized release, disclosure, and dissemination to the world of
22 Plaintiffs’ and Class Members’ PII/PHI for no lawful purpose.

23 138. Sony, by and through its above negligent or grossly negligent actions, inaction,
24 omissions, and want of ordinary care, unlawfully breached its duties to Plaintiffs and Class
25 Members by, among other things, failing to exercise reasonable care in safeguarding and
26 protecting Plaintiffs’ and Class Members’ PII/PHI within its possession, custody and control.

27 139. Sony, by and through its above negligent or grossly actions, inaction,
28 omissions, and want of ordinary care, further breached its duties to Plaintiffs and Class

1 Members by failing to design, adopt, implement, control, direct, oversee, manage, monitor and
2 audit its processes, controls, policies, procedures, protocols, and software and hardware
3 systems for complying with the applicable laws and safeguarding and protecting their PII/PHI.

4 140. But for Sony's negligent or grossly negligent breach of the above-described
5 duties owed to Plaintiffs and Class Members, their PII/PHI would not have been released,
6 disclosed, and disseminated to the world – without their authorization – and compromised.

7 141. Plaintiffs' and Class Members' PII/PHI was transferred, sold, opened, viewed,
8 mined and otherwise released, disclosed, and disseminated to the world via, among other
9 things, publication on the Internet, without their authorization as the direct and proximate
10 result of Sony's failure to design, adopt, implement, control, direct, oversee, manage, monitor
11 and audit its processes, controls, policies, procedures and protocols for complying with the
12 applicable laws and safeguarding and protecting Plaintiffs' and Class Members' PII/PHI.

13 142. Sony's above-described wrongful actions, inaction, omissions, and want of
14 ordinary care that directly and proximately caused the Data Breach constitute negligence,
15 gross negligence, and negligence *per se* under California common law.

16 143. As a direct and proximate result of Sony's above-described wrongful actions,
17 inaction, omissions, and want of ordinary care that directly and proximately caused the Data
18 Breach, Plaintiffs and Class Members have suffered (and will continue to suffer) economic
19 damages and other injury and actual harm in the form of, *inter alia*, (i) actual identity theft,
20 identity fraud or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of
21 their PII/PHI, (iv) statutory nominal damages of \$1000 per Plaintiff and each Class Member
22 under the CMIA (CAL. CIV. CODE § 56.36(b)(1)), (v) expenses and losses in discharging their
23 duties (CAL. LAB. CODE §§ 2800 and 2802), (vi) deprivation of the value of their PII/PHI, for
24 which there is a well-established national and international market, (vii) the financial and
25 temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating
26 their damages (*see above*), and (viii) the imminent, immediate and continuing increased risk of
27 identity theft, identity fraud or medical fraud – for which they are entitled to compensation.
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
COUNT VI**BREACH OF CONFIDENTIALITY****(On Behalf of Plaintiffs and Each Class Member)**

144. The preceding factual statements and allegations are incorporated by reference.

145. Plaintiffs' and Class Members' unique, personal, and private PII/PHI in Sony's possession, custody, and control was (and continues to be) highly confidential.

146. Sony breached the confidentiality of Plaintiffs' and Class Members' PII/PHI by failing to identify, implement, maintain and monitor appropriate data security measures, policies, procedures, protocols, and/ software and hardware systems to ensure the security and confidentiality of Plaintiffs' and Class Members' PII/PHI, and wrongfully releasing and disclosing their PII/PHI without authorization, as described above.

147. Had Sony not engaged in the above-described wrongful actions, inaction and omissions, the Data Breach never would have occurred and Plaintiffs' and Class Members' PII/PHI would not have been wrongfully released, disclosed, compromised, disseminated to the world, and wrongfully used. Sony's wrongful conduct constitutes (and continues to constitute) the tort of breach of confidentiality at California common law.

148. As a direct and proximate result of Sony's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) actual identity theft, identity fraud or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory nominal damages of \$1000 per Plaintiff and each Class Member under the CMIA (CAL. CIV. CODE § 56.36(b)(1)), (v) expenses and losses in discharging their duties (CAL. LAB. CODE §§ 2800 and 2802), (vi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, (vii) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages (*see above*), and (viii) the imminent, immediate and continuing increased risk of identity theft, identity fraud and medical fraud – for which they are entitled to compensation.

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

COUNT VII

INDEMNIFICATION

(CAL. LAB. CODE §§ 2800 and 2802)

(On Behalf of Plaintiffs and Each Sony Employee Sub-Class Member)

149. The preceding factual statements and allegations are incorporated by reference.

150. Under CAL. LAB. CODE § 2800, an employer must indemnify its current and former employees for losses caused by the employer’s want of ordinary care.

151. Under CAL. LAB. CODE § 2802(a), an employer also must indemnify its current and former employees for all necessary expenditures or losses incurred by the employees in directly discharging their duties, or in obedience to the employer’s directions, even though unlawful, unless the employee, at the time of his or her obedience, believed them to be unlawful.

152. Sony required its current and former employees, including Plaintiffs and Sony Employee Sub-Class Members, to provide their confidential and personal PII/PHI as a condition of employment. Sony, however, failed to safeguard and protect their PII/PHI by failing to identify, implement, maintain and monitor appropriate data security measures, policies, procedures, protocols, and software and hardware systems which, in turn, directly and proximately caused the Data Breach, and the unauthorized release, disclosure, and dissemination to the world of their PII/PHI.

153. As a direct and proximate result of Sony’s above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiffs and Sony Employee Sub-Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) actual identity theft, identity fraud or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory nominal damages of \$1000 per Plaintiff and each Class Member under the CMIA (CAL. CIV. CODE § 56.36(b)(1)), (v) expenses and losses in discharging their duties (CAL. LAB. CODE §§ 2800 and 2802), (vi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, (vii) the

1 financial and temporal cost of monitoring their credit, monitoring their financial accounts, and
2 mitigating their damages (*see* above), and (viii) the imminent, immediate and continuing
3 increased risk of identity theft, identity fraud or medical fraud – for which they are entitled to
4 compensation.

5 154. Sony has intentionally and willfully failed and refused to reimburse Plaintiffs
6 and Sony Employee Sub-Class Members for such losses and expenses.

7 155. Plaintiffs and Sony Employee Sub-Class Members, therefore, are entitled to
8 recover such losses and expenses incurred during the course and scope of their employment,
9 plus attorneys' fees, litigation expenses, costs, and interest under CAL. LAB. CODE §§ 2800 and
10 2802.

11 **COUNT VIII**

12 **UNJUST ENRICHMENT/ASSUMPSIT**

13 **(On Behalf of Plaintiffs and Each Class Member)**

14 156. The preceding factual statements and allegations are incorporated by reference.

15 157. By its above-described wrongful actions, inaction, omissions, and want of
16 ordinary care that directly and proximately caused the Data Breach – to wit, Sony's failure to
17 identify, implement, maintain and monitor the proper data security measures, policies,
18 procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs'
19 and Class Members' PII/PHI – Sony has been (and continues to be) unjustly enriched by, *inter*
20 *alia*, (i) the saved cost of implementing the proper PII/PHI security measures, policies,
21 procedures, protocols, and software and hardware systems in its computer system and servers,
22 that it did not implement, (ii) the shifted risk and expense of the Data Breach to Plaintiffs and
23 Class Members, and (iii) the return on investment on all above-described amounts.

24 158. Sony, therefore, should be compelled to refund (or disgorge) such wrongfully
25 collected, saved back and shifted funds and expenses under the California common law
26 equitable doctrine of unjust enrichment and the duty to make restitution under the California
27 common law equitable doctrine of assumpsit.

28

RELIEF REQUESTED

159. The preceding factual statements and allegations are incorporated by reference.

160. **DAMAGES.** As a direct and proximate result of Sony's wrongful actions, inaction, omissions, and want of ordinary care (as described above) that directly and proximately caused the Data Breach which, on information and belief, occurred entirely within the State of California, Plaintiffs and Class Members suffered (and will continue to suffer) actual, consequential, incidental, and statutory damages and other injury and harm in the form of, *inter alia*, (i) actual identity theft, identity fraud or medical fraud, (ii) invasion of privacy, (iii) breach of the confidentiality of their PII/PHI, (iv) statutory nominal damages of \$1000 per Plaintiff and each Class Member under the CMIA (CAL. CIV. CODE § 56.36(b)(1)), (v) expenses and losses in discharging their duties (CAL. LAB. CODE §§ 2800 and 2802), (vi) deprivation of the value of their PII/PHI, for which there is a well-established national and international market, (vii) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages (*see* above), and (viii) the imminent, immediate and continuing increased risk of identity theft, identity fraud or medical fraud – for which they are entitled to compensation. Plaintiffs and Class Members also are entitled to equitable relief, including, without limitation, disgorgement and restitution. Plaintiffs' and Class Members' damages were foreseeable by Sony and exceed the minimum jurisdictional limits of this Court. All conditions precedent to Plaintiffs' and Class Members' claims have been performed and occurred.

161. **PUNITIVE DAMAGES.** Plaintiffs and Class Members also are entitled to punitive damages from Sony, as punishment and to deter such wrongful conduct in the future, pursuant to, *inter alia*, CAL. CIV. CODE § 56.35 and California common law. All conditions precedent to Plaintiffs' and Class Members' claims have been performed and occurred.

162. **INJUNCTIVE RELIEF.** Pursuant to, *inter alia*, CAL. CIV. CODE § 56.35 and CAL. BUS. & PROF. CODE § 17203, Plaintiffs and Class Members also are entitled to injunctive relief in multiple forms including, without limitation, (i) credit monitoring, (ii) internet monitoring, (iii) identity theft insurance, (iv) prohibiting Sony from continuing its above-described

1 wrongful conduct, (v) requiring Sony to modify its corporate culture and design, adopt,
2 implement, control, direct, oversee, manage, monitor, and audit appropriate data security
3 processes, controls, policies, procedures, protocols, and software and hardware systems to
4 safeguard and protect the PII/PHI entrusted to it, (vi) periodic compliance audits by a third
5 party to insure that Sony is properly safeguarding and protecting the PII/PHI in its possession,
6 custody and control, and (vii) clear and effective notice to Class Members about the serious
7 risks posed by the theft of the PII/PHI and the precise steps that must be taken to protect
8 themselves. All conditions precedent to Plaintiffs' and Class Members' claims for relief have
9 been performed and occurred.

10 163. **ATTORNEYS' FEES, LITIGATION EXPENSES AND COSTS.** Plaintiffs and Class
11 Members also are entitled to recover their attorneys' fees, litigation expenses and court costs in
12 prosecuting this action pursuant to, *inter alia*, CAL. CIV. CODE § 56.35 and CAL. LAB. CODE §§
13 2800 and 2802. All conditions precedent to Plaintiffs' and Classes' claims for relief have been
14 performed and occurred.

15 **WHEREFORE**, Plaintiffs, on behalf of themselves and Class Members, respectfully
16 request that (i) this action be certified as a class action, (ii) Plaintiffs be designated Class
17 Representatives, and (iii) Plaintiffs' Counsel be appointed as Class Counsel. Plaintiffs, on
18 behalf of themselves and Class Members, further request that upon final trial or hearing,
19 judgment be awarded against Sony for:

- 20 (i) actual, incidental, consequential, and nominal damages to be determined by the
21 trier of fact;
- 22 (ii) statutory damages (as set forth above);
- 23 (iii) punitive damages (as set forth above);
- 24 (iv) equitable relief, including restitution, disgorgement of all amounts by which Sony
25 has been unjustly enriched (as set forth above);
- 26 (v) pre- and post-judgment interest at the highest legal rates applicable;
- 27 (vi) appropriate injunctive relief (as set forth above);
- 28 (vii) attorneys' fees and litigation expenses;

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

- (viii) costs of suit; and
- (ix) such other and further relief that the Court deems just and proper.

JURY DEMAND

Plaintiffs, on behalf of themselves and all others similarly situated, respectfully demand a trial by jury on all of their claims and causes of action so triable.

Dated: February 24, 2015

BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
THOMAS J. O'REARDON II (247952)

By: Timothy Blood /r
TIMOTHY G. BLOOD

701 B Street, Suite 1700
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
toreardon@bholaw.com

CADENA CHURCHILL
RAUL CADENA (185787)
701 B Street, Suite 1700
San Diego, CA 92101
Tel: 619/546-0888
619/923-3208 (fax)
rcadena@cadenachurchill.com

THE COFFMAN LAW FIRM
RICHARD L. COFFMAN (*pro hac vice to be filed*)
First City Building
505 Orleans St., Suite 505
Beaumont, TX 77701
Tel: 409/833-7700
866/835-8250 (fax)
rcoffman@coffmanlawfirm.com

BARNOW AND ASSOCIATES, P.C.
BEN BARNOW (*pro hac vice to be filed*)
One North LaSalle Street, Suite 4600
Chicago, IL 60602
Tel: 312/621/2000
312/641-5504 (fax)
b.barnow@barnowlaw.com

LAW OFFICES OF CAMERON J.
GHARABIKLOU
CAMERON J. GHARABIKLOU (249189)
530 B Street, Suite 1530

San Diego, CA 92101
Tel: 858/412-0019
619/568-3341 (fax)
cameron@justice-lawgroup.com
Attorneys for Plaintiffs and the Putative Class

BLOOD HURST & O'REARDON, LLP

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

Attachment A to
Class Action Complaint



10202 West Washington Boulevard
Culver City, California 90232-3195

December 8, 2014

Dear SPE Employee:

Sony Pictures Entertainment ("SPE") is writing to provide you with a summary of SPE's prior communications regarding the significant system disruption SPE experienced on Monday, November 24, 2014, as well as to provide you with additional detail.

As you know, SPE has determined that the cause of the disruption was a brazen cyber attack. After identifying the disruption, SPE took prompt action to contain the cyber attack, engaged recognized security consultants and contacted law enforcement.

SPE learned on December 1, 2014, that the security of personally identifiable information that SPE received about you and/or your dependents during the course of your employment may have been compromised as a result of such brazen cyber attack. Although SPE is in the process of investigating the scope of the cyber attack, SPE believes that the following types of personally identifiable information that you provided to SPE may have been obtained by unauthorized individuals: (i) name, (ii) address, (iii) social security number, driver's license number, passport number, and/or other government identifier, (iv) bank account information, (v) credit card information for corporate travel and expense, (vi) username and passwords, (vii) compensation and (viii) other employment related information. In addition, unauthorized individuals may have obtained (ix) HIPAA protected health information, such as name, social security number, claims appeals information you submitted to SPE (including diagnosis and disability code), date of birth, home address, and member ID number to the extent that you and/or your dependents participated in SPE health plans, and (x) health/medical information that you provided to us outside of SPE health plans.

As SPE previously notified you, SPE has made arrangements with a third-party service provider, AllClear ID, to offer all employees and dependents twelve (12) months of identity protection services at no charge. As a reminder, to obtain credit monitoring and identity theft insurance, you will need to enroll. On Wednesday, December 3, 2014, you received an email from SonyPictures@AllClearID.com. This email contained your unique, nontransferable activation code for enrolling in the AllClear identity theft protection services. In addition, since December 3, 2014, you have had access to identity repair assistance. AllClear ID's multi-language call center is available to respond to your questions and assist you Monday-Saturday, from 8 am to 8 pm CST. You may also email AllClear ID's support center at support@allclearid.com.

For your security SPE encourages you to be especially aware of email, telephone, and postal mail scams that ask for personal or sensitive information. Neither SPE nor anyone acting on its behalf will contact you in any way, including by email, asking for your credit card number, social security number or other personally identifiable information. If you are asked for this information, you can be confident SPE is not the entity asking. To protect against possible identity theft or other financial loss, SPE encourages you to remain vigilant, review your account statements, monitor your credit reports and change your passwords. SPE is providing the following information for those who wish to consider it:

- You may wish to visit the web site of the U.S. Federal Trade Commission at <http://www.consumer.ftc.gov/features/feature-0014-identity-theft> or reach the FTC at 1-877-382-4357 or 600 Pennsylvania Avenue, NW, Washington, DC 20580 for further information about how to protect yourself from identity theft. Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, and the FTC.
- U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free (877) 322-8228.
- You can request information regarding "fraud alerts" and "security freezes" from the three major U.S. credit bureaus are listed below. At no charge, if you are a U.S. resident, you can have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. This service can make it more difficult for someone to get credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it also may delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. A "security freeze" generally prohibits the credit reporting agency from releasing your credit report or any information from it without your written authorization. You should be aware that placing a security freeze on your credit account may delay or interfere with the timely approval of any requests that you make for new loans, credit mortgages, or other services. Unlike fraud alerts, to obtain a security freeze you must send a written request to each of the three major reporting agencies. Should you wish to place a fraud alert or a security freeze, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.
 - Experian: (888) 397-3742; www.experian.com; P.O. Box 9532, Allen, TX 75013
 - Equifax: (800) 525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
 - TransUnion: (800) 680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Please contact us at (855) 731-6013 should you have any additional questions.