BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
THOMAS J. O'REARDON II (247952)
PAULA M. ROACH (254142)
701 B Street, Suite 1700
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
toreardon@bholaw.com
proach@bholaw.com

Attorneys for Plaintiffs Bruce Ochmanek, Hiram Vargas, and the Putative Class

[Additional Counsel Appear on Signature Page]

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF LOS ANGELES –CENTRAL CIVIL WEST

SUSAN DUKOW, *et al*., on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

SONY PICTURES ENTERTAINMENT, INC.,

Defendant.

Case No. BC566884

CLASS ACTION

CONSOLIDATED AMENDED CLASS AND REPRESENTATIVE ACTION COMPLAINT

BY FAX

Dept: 311
Judge: Hon. John S. Wiley

Date Filed: December 16, 2014
Trial Date: TBD

JURY TRIAL DEMANDED

Pursuant to the Court's Initial Status Conference Ruling consolidating the four related actions into Case No. BC566884, Plaintiffs Susan Dukow, Sherrill Perryman, L. Churchill, Amy McKenzie, Bruce Ochmanek, and Hiram A. Vargas (collectively, "Plaintiffs"), on behalf of themselves and all others similarly situated, and Plaintiff Vargas also as a representative of all aggrieved employees, file this Consolidated Amended Class and Representative Action Complaint against Defendant Sony Pictures Entertainment, Inc. ("Sony", "SPE" or "Defendant"), and respectfully allege the following:

NATURE OF THE ACTION

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

2. In November 2014, Sony betrayed Plaintiffs' and Class Members' trust by failing to properly safeguard and protect their PII/PHI, thereby publicly disclosing their PII/PHI without authorization (*i.e.*, the "Data Breach" or "Breach") in violation of numerous laws, including, *inter alia*, the California Confidentiality of Medical Information Act ("CMIA") (CAL. CIV. CODE § 56, *et seq.*), California Unfair Competition Law (CAL. BUS. & PROF. CODE § 17200, *et seq.*), California Security Requirements for Consumer Records (CAL. CIV. CODE §§ 1798.29 and 1798.80, *et seq.*), California Labor Code §§ 2800 and 2802 (indemnification), Article 1, § 1 of the California Constitution, the California Private Attorneys General Act of 2004 (CAL. LAB. CODE § 2698, *et seq.*) ("PAGA"), and California common law.

3. On or about December 2, 2014, after reports began surfacing on the Internet, Sony announced that on November 24, 2014, it learned that Plaintiffs' and Class Members'

PII/PHI had been unlawfully released, disclosed, and disseminated to the world without their authorization (*i.e.*, the "Data Breach").

4. The wrongfully released and disclosed PII/PHI included, *inter alia*, Plaintiffs' and Class Members' (i) names, (ii) addresses, (iii) Social Security numbers, driver license numbers, passport numbers, or other government identifiers, (iv) bank account information, (v) credit card information for corporate travel and expense, (vi) usernames and passwords, (vii) compensation, (viii) other employment-related information, (ix) health information protected by law, such as names, Social Security numbers, claims appeals information submitted to Sony (including diagnoses and disability codes), dates of birth, home addresses, and Sony health plan member ID numbers, and (x) health/medical information provided to Sony outside of the Sony health plans. In a December 8, 2014 Data Breach Notification Letter (Exhibit A), Sony confirmed to Plaintiffs and Class Members that the above-referenced information had been released and disclosed without their authorization.

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

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

7. Plaintiffs are concerned about their finances, credit, identities, medical records, and PII/PHI and, as such, regularly monitor their credit, regularly monitor their financial

accounts and/or carefully store and dispose of their PII/PHI and other documents containing their PII/PHI. Since the Data Breach, Plaintiffs and Class Members have experienced identity theft,[1] identity fraud, medical fraud,[2] lost medical identities and records, fraudulent credit card activity, opening new credit card accounts in their name, phishing scams,[3] increased mailers marketing products and services including, *inter alia*, medical products, medical services or prescription drugs specifically targeted to their medical conditions, and the imminent, immediate or continuing increased risk of identity theft, identity fraud or medical fraud.

8. Plaintiffs have standing to bring this suit because as a direct and proximate result of Sony's wrongful actions, inaction, omissions, and want of ordinary care, and the resulting Data Breach, they 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

[1] According to the United States Government Accounting Office (GAO), the terms "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).

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

[3] "Phishing" is an attempt to acquire information (and sometimes, indirectly, money), such as usernames, passwords and credit card details by masquerading as a trustworthy entity through an electronic communication. Communications purporting to be from popular social websites, auction sites, online payment processors or IT administrators are commonly used to lure the unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by e-mail spoofing or instant messaging, and 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.

well-established national and international market,[4] (vii) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages (*see* below), (viii) the imminent, immediate and continuing increased risk of identity theft, identity fraud or medical fraud – for which they are entitled to compensation, and (ix) civil penalties under the PAGA (CAL. LAB. CODE § 2698, *et seq.*).

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

JURISDICTION AND VENUE

10. This Court has jurisdiction over this matter pursuant to the California Constitution, Article XI, § 10 and California Code of Civil Procedure ("CCP") § 410.10, because Sony transacted business and committed the acts alleged in California. More than two-thirds (*i.e.*, 100%) of the Class Members are California citizens, the sole defendant is

---

[4] PII/PHI is a valuable property right. *See, e.g.*, John T. Soma, *et al*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-*4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of 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 provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected." *See* Federal Trade Commission, *Medical Identity Theft*, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited March 27, 2014). Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use compromised PHI to adjust their insureds' medical insurance premiums.

The value of PHI as a commodity also is measurable. *See, e.g.*, Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market* (April 28, 2014), http://www.medscape.com/viewarticle/824192 (last visited June 26, 2014); Adam Greenberg, *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-the-online-black-market/article/303302/ (last visited June 26, 2014).

located in California, and Sony has its principal place of business, and is headquartered, in California; thus, this case is not subject to removal under the Class Action Fairness Act of 2005 because it falls under both the "home state exception" and the "local controversy exception." 28 U.S.C. § 1332(d)(4)(A) (home state exception); 28 U.S.C. § 1332 (d)(4)(B) (local controversy exception).

11. Venue is appropriate in Los Angeles County because Plaintiffs reside in Los Angeles County and Sony, which is headquartered in Los Angeles County, did, and is doing business in Los Angeles County.

PARTIES

12. Plaintiff Susan Dukow ("Dukow") is a citizen and resident of Los Angeles County, California, who previously was employed by Sony in various production jobs on various motion pictures. In connection with her employment, Dukow entrusted Sony with her most sensitive personal and medical information (*i.e.*, her PII/PHI) which, pursuant to law, Sony was (and continues to be) required to safeguard, protect, and keep confidential. Sony, however, failed to do so. Dukow's PII/PHI was stored on the unprotected server hacked by the group known as the "Guardians of Peace" on or about November 24, 2014, and exposed to the world. Thereafter, one or more data thieves and their subsequent customers transferred, sold, opened, read, mined and otherwise used Dukow's PII/PHI, without her authorization, to their financial benefit and her financial detriment. Since the Data Breach, Dukow has spent numerous hours monitoring her credit and financial accounts for fraudulent activity. As a direct and proximate result of Sony's wrongful actions, inaction, omissions, and want of ordinary care, and the resulting Data Breach, Dukow has suffered (and will continue to suffer) the above-described economic damages and other injury and actual harm. Sony's unauthorized and wrongful release and disclosure of Dukow's PII/PHI also placed her at an imminent, immediate, and continuing increased risk of injury and harm from identity theft, identity fraud, and medical fraud.

13. Plaintiff Sherrill Perryman ("Perryman") is a citizen and resident of Ventura, California, who previously was employed by Sony as a production coordinator. In connection

with her employment, Perryman entrusted Sony with her most sensitive personal and medical information (*i.e.*, her PII/PHI) which, pursuant to law, Sony was (and continues to be) required to safeguard, protect, and keep confidential. Sony, however, failed to do so. Perryman's PII/PHI was stored on the unprotected server hacked by the group known as the "Guardians of Peace" on or about November 24, 2014, and exposed to the world. Thereafter, one or more data thieves and their subsequent customers transferred, sold, opened, read, mined and otherwise used Perryman's PII/PHI, without her authorization, to their financial benefit and her financial detriment. Since the Data Breach, Perryman has spent numerous hours monitoring her credit and financial accounts for fraudulent activity. As a direct and proximate result of Sony's wrongful actions, inaction, omissions, and want of ordinary care, and the resulting Data Breach, Perryman has suffered (and will continue to suffer) the above-described economic damages and other injury and actual harm. Sony's unauthorized and wrongful release and disclosure of Perryman's PII/PHI also placed her at an imminent, immediate, and continuing increased risk of injury and harm from identity theft, identity fraud, and medical fraud.

14. Plaintiff L. Churchill ("Churchill"), previously identified as Jane Doe, is a citizen and resident of Los Angeles County, California, who previously was employed by Sony in social media marketing. In connection with her employment, Churchill entrusted Sony with her most sensitive personal and medical information (*i.e.*, her PII/PHI) which, pursuant to law, Sony was (and continues to be) required to safeguard, protect, and keep confidential. Sony, however, failed to do so. Churchill's PII/PHI was stored on the unprotected server hacked by the group known as the "Guardians of Peace" on or about November 24, 2014, and exposed to the world. Thereafter, one or more data thieves and their subsequent customers transferred, sold, opened, read, mined and otherwise used Churchill's PII/PHI, without her authorization, to their financial benefit and her financial detriment. Since the Data Breach, Churchill has spent numerous hours monitoring her credit and financial accounts for fraudulent activity. As a direct and proximate result of Sony's wrongful actions, inaction, omissions, and want of ordinary care, and the resulting Data Breach, Churchill has

suffered (and will continue to suffer) the above-described economic damages and other injury and actual harm. Sony's unauthorized and wrongful release and disclosure of Churchill's PII/PHI also placed her at an imminent, immediate, and continuing increased risk of injury and harm from identity theft, identity fraud, and medical fraud.

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

16. Plaintiff Bruce Ochmanek ("Ochmanek") is a citizen and resident of Los Angeles, California, who previously was employed by Sony. In connection with his employment, Ochmanek entrusted Sony with his most sensitive personal and medical information (*i.e.*, his PII/PHI) which, pursuant to law, Sony was (and continues to be) required to safeguard, protect, and keep confidential. Sony, however, failed to do so, which Sony confirmed to Ochmanek in its Data Breach Notification Letter. In the letter, Sony confirmed

that his PII/PHI was stored on the unprotected server hacked by the group known as "Guardians of Peace" on or about November 24, 2014, and exposed to the world. Thereafter, one or more data thieves and their subsequent customers transferred, sold, opened, read, mined and otherwise used Ochmanek's PII/PHI, without his authorization, to their financial benefit and his financial detriment. Since the Data Breach, Ochmanek has spent numerous hours monitoring his credit and financial accounts for fraudulent activity. As a direct and proximate result of Sony's wrongful actions, inaction, omissions, and want of ordinary care, and the resulting Data Breach, Ochmanek has suffered (and will continue to suffer) the above-described economic damages and other injury and actual harm. Sony's unauthorized and wrongful release and disclosure of Ochmanek's PII/PHI also placed him at an imminent, immediate, and continuing increased risk of injury and harm from identity theft, identity fraud, and medical fraud.

17. Plaintiff Hiram A. Vargas ("Vargas") is a citizen and resident of Los Angeles, California, who was employed by Sony until February 26, 2014. In connection with his employment, Vargas entrusted Sony with his most sensitive personal and medical information (*i.e.,* his PII/PHI) which, pursuant to law, Sony was (and continues to be) required to safeguard, protect, and keep confidential. Sony, however, failed to do so, which Sony confirmed to Vargas in its Data Breach Notification Letter. In the letter, Sony confirmed that his PII/PHI was stored on the unprotected server hacked by the group known as "Guardians of Peace" on or about November 24, 2014, and exposed to the world. Thereafter, one or more data thieves or their subsequent customers transferred, sold, opened, read, mined or otherwise used Vargas' PII/PHI, without his authorization, to their financial benefit and his financial detriment. Since the Data Breach, Vargas has spent numerous hours monitoring his credit and financial accounts for fraudulent activity. As a direct and proximate result of Sony's wrongful actions, inaction, omissions, and want of ordinary care, and the resulting Data Breach, Vargas has suffered (and will continue to suffer) the above-described economic damages and other injury and actual harm. Sony's unauthorized and wrongful release and disclosure of Vargas'

PII/PHI also placed him at an imminent, immediate, and continuing increased risk of injury and harm from identity theft, identity fraud, and medical fraud.

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

FACTS

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

19. On November 24, 2014, hackers calling themselves the Guardians of Peace infiltrated and disrupted Sony's internal computer systems and networks (the "Data Breach").

20. Thereafter, on December 2, 2014, the Guardians of Peace published online Plaintiffs' and Class Members' PII/PHI released and disclosed by Sony to the Guardians of Peace as part of the Data Breach – including Plaintiffs' and Class Members' 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.

21. Also on December 2, 2014, noted data security blogger Brian Krebs reported on his website, Krebs on Security (www.krebsonsecurity.com), that more than 25 gigabytes of sensitive data (PII) 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 had been released and disclosed to the hackers. *See* http://krebsonsecurity.com/page/3/ (last visited January 2, 2015). The hackers also may have destroyed data on an unknown number of Sony's internal computer systems and networks. *Id*.

22. 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 pertained to an internal audit performed by PriceWaterhouse Coopers that includes screen shots of dozens of Sony employee federal tax records and other compensation data. *Id.*

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

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

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

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

26. On December 8, 2014, Sony formally notified Plaintiffs and Class Members about the Data Breach, confirming that the security of their PII/PHI and their dependents' PII/PHI that Sony received from them during the course of their employment – including: (i) names, (ii) addresses, (iii) Social Security numbers, driver license numbers, passport numbers, or other government identifiers, (iv) bank account information, (v) credit card information for corporate travel and expense, (vi) usernames and passwords, (vii) compensation, and (viii) other employment-related information – had been released, disclosed, and compromised without their authorization as part of the Data Breach. *Id*. *See* exemplar of uniform December 8, 2014 Data Breach Notification Letter sent to Plaintiffs and Class Members (Exhibit A).

27. Sony also confirmed in the Data Breach Notification Letter that Plaintiffs' and Class Members' PHI – including: (i) health/medical information required to be protected by law, such as names, Social Security numbers, claims appeals information submitted to Sony (including diagnoses and disability codes), dates of birth, home addresses, and Sony health plan member ID numbers, and (ii) health/medical information provided to Sony outside of the

Sony health plans – had been released, disclosed, and compromised without their authorization as part of the Data Breach.. *Id*.

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

29. The Data Breach Notification Letters also squarely placed the burden on Plaintiffs and Class Members, rather than Sony, to protect themselves and mitigate their Data Breach damages – such as reviewing their account statements, monitoring their credit reports, and changing their passwords. *Id.* Unfortunately, many of Sony's mitigation directives required Plaintiffs and Class Members to incur additional out-of-pocket expenses. For example, as a general rule in California, the fee to place (and remove) a "security freeze" on one's credit report, as suggested by the Data Breach Notification Letters, is $10 each time it is placed at each of the three credit reporting agencies (Experian, Equifax, and TransUnion). Monitoring one's credit reports, another option suggested by the Data Breach Notification Letters, would cause a Data Breach victim to incur an expense to see his or her credit reports beyond the one free annual report to which they are entitled.

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

31. The Data Breach Notification Letters also notified Plaintiffs and Class Members that Sony would provide one year of free credit monitoring and identity theft

insurance to all affected persons who take more time away from their businesses and families to enroll. The offered "data security package," however, is inadequate At best, the credit monitoring service is an indirect manner of tracking identity theft – it may reveal new financial accounts opened with compromised PII/PHI, but does nothing to prevent unauthorized charges made to existing payment card accounts. The PII/PHI "protection" offered by Sony also is woefully inadequate because, *inter alia*:

(i) The free credit monitoring and identity theft insurance offered by Sony is only for one year. As advised by the Federal Trade Commission, however, a person impacted by a data breach should take proactive steps well after a year has passed to protect against identity theft and related fraud;

(ii) Sony offered only a single bureau credit monitoring program – as opposed to the industry recommended triple bureau program – that provides no protection to minors. Each minor child victim continues to be fully exposed to damages; and

(iii) Sony did not provide any protection against medical identity theft and 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 (last visited August 12, 2014).

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

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

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

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

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

36. The ensuing scandal was huge, attracting attention from the Bush Administration. The FTC also got involved. Several lawsuits were filed accusing Sony of trading in malicious software and violating users' rights – which Sony settled. Meanwhile, the debacle angered the hacker community. The rootkit scandal is arguably the Big Bang moment for Sony's cybersecurity troubles because when hackers get angry, they tend to hold a grudge.

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

38. In an inadequate attempt to close the barn door after the horse got out, Sony released a firmware update to patch the exploit, though other hackers followed Hotz's lead and were ultimately able to run any software, including Linux, on a PlayStation 3.[5] In January 2011, Hotz released the console's root keys for further hacking opportunities.

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

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

41. Within two weeks of its warning, Anonymous took down the PlayStation Network. The Network stayed down for twenty-three days, during which Anonymous also obtained the PII of 77 million PlayStation accountholders. The attack ended up costing Sony at least $171 million. The hackers had sent a clear message. Then, the floodgates opened.

42. Following the Anonymous attack, Sony was attacked relentlessly. By one security firm's count, there were twenty-one major incidents in the six months following the initial PlayStation Network outage. Some of the attacks were relatively harmless breaches of Sony's unprotected international websites, principally targeting Sony BMG and other music-related businesses. Some of the websites were defaced. Some were taken offline completely. Some data was released, disclosed, and compromised without authorization.

43. But some of the system breaches following the devastating Sony PlayStation Network breach were historically devastating in their own right. For example, in a June 2011 data breach of Sony Pictures' unprotected servers, secured private information, including passwords and home addresses, of over 1,000,000 accounts was released and disclosed to

[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.

hacker LulzSec. The hackers boasted on the Internet that the data was unencrypted. Passwords were just sitting there in plain text – much like in this case where Sony openly stored thousands of passwords in a folder named "Password." Again, Sony did nothing.

44. The data breaches kept occurring. Although some data security experts thought the breaches were an inside job since Sony fired a slew of employees from the department that is supposed to guard the company from cyberattacks, it seems more likely that the fired employees were just bad at their jobs.

45. For example, after the unprotected computer systems of a Sony division in one country would be breached, Sony would not change a thing to protect the rest of its interests, and then a week later, unprotected computer systems of another Sony division in another country were breached in the exact same manner. It is even more astonishing that Sony still had not secured its internal computer systems and network, and suffered the recent company-wide Data Breach giving rise to this action. But that is exactly what happened – the Guardians of Peace have proven that Sony left its internal computer systems and entire network unprotected and vulnerable to a single – albeit massive – data breach that released and disclosed Plaintiffs' and Class Members' PII/PHI without their authorization.

46. In February 2014, Jason Spaltro ("Spaltro"), then the Executive Director of Information Security at SPE, notified Sony Chief Financial Officer David Hendler that a significant amount of payment card information pertaining to 759 individuals in Brazil had been released and disclosed to fraudsters by Sony's internal computer systems and network. The compromised payment card information had been stored as .txt text files in a manner in which Sony had stored this type of information since 2008. Spaltro, however, brushed off the significance of the February 2014 data breach, recommending against notifying the victims that it had occurred.

47. In August 2014, a month after Sony settled the PlayStation class action litigation resulting from the April 2011 data breach, hackers again took down the unprotected PlayStation Network and Sony's Entertainment Network by overwhelming the networks with "denial of service" attacks. Also in August 2014, ARS Technica, an online information

technology publication, reported that, upon resigning as Sony's Chief Information Security Officer, Phil Reitinger remarked that there are a number of archaic systems that had been in place at Sony for ages with plenty of potential attack points.

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

49. The core of Sony's problem is that its cybersecurity is totally inadequate. The situation is further exacerbated by its corporate culture and flippant attitude towards protecting its current and former employees' and independent contractors' PII/PHI. Indeed, Spaltro made a business decision in November 2005 not to ensure the security of Sony's internal computer systems and network, even though he was warned by an auditor who had just completed a review of Sony's cybersecurity practices that Sony had several security weaknesses, including insufficiently strong access controls, which is a key Sarbanes-Oxley requirement. Spaltro subsequently stated in a 2007 interview with the business website CIO that he was not willing to put up a lot of money to safeguard and protect Sony's sensitive information because "[i]t's a valid business decision to accept the risk." CIO subsequently reported that Ari Schwartz, a privacy expert with the Center for Democracy and Technology, believed Spaltro's reasoning to be "shortsighted" because the cost of notification is only a small portion of the potential cost of a data breach. Spaltro's business decision continues to haunt Sony to this day.

50. Sony's systemic and systematic pattern of internal computer systems and network security failures and data breaches confirm its knowing unwillingness, failure, and refusal to correct its faulty data protection policies. Sony knew its data security processes, controls, policies, procedures, protocols, and software and hardware systems were insufficient, antiquated, inadequate, and did not safeguard and protect its current and former employees' and independent contractors' PII/PHI, yet did nothing to expand, improve or update them. On information and belief, Sony's pattern of willful and intentional disregard of the security of its current and former employees' and independent contractors' PII/PHI in its possession and control – which directly and proximately caused the Data Breach – continues notwithstanding

the repeated warnings it has received, the repeated data breaches it has suffered, and the repeated embarrassment heaped upon it.

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

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

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

53. The Data Breach could have been prevented had Sony properly addressed its organizational issues after the 2011 PlayStation Network breach. Sony admittedly operated as a collection of silos. Sony should have immediately instituted a cybersecurity sharing and collaboration solution between their divisions and their supply chain. From 2011 forward, Sony should have implemented standardized corporate-wide cybersecurity and beefed up employee information security training across the organization. The tools and techniques Sony decided to use to protect the unprotected PlayStation Network were a reactive approach – Sony was attacked at point X by Y, so it defended point X with tools to stop successful exploitation by those kinds of Y attacks. It was completely reactive, but not proactive. More importantly, it did not work. *See* December 25, 2014 PlayStation Network breach (above).

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

55. The Data Breach also could have been prevented had Sony used minimum industry standards, such as adequate passwords. The password "password," which was used by Sony in three certificates, was used by the hackers to digitally sign the malware they installed in Sony's computer systems and networks. Sony also used weak passwords to protect internal and Internet-facing critical servers within its computer systems and network.

56. The Data Breach also could have been prevented had Sony conducted regular data security assessments. Sony failed to detect weak passwords and failed to prevent the massive Data Breach. Most companies – such as Sony – treat the investment in cybersecurity as an optional expense. Sony should have conducted penetration tests on a regular basis, using both automated pen-testing tools and manual security checks. Sony, however, took the easy way out with its security testing.

57. The Data Breach also could have been prevented had Sony installed the proper computer system and network alarms, and properly monitored its systems and networks. Numerous alarms should have been triggered while the computer systems and networks were being breached and compromised. These notifications would have allowed Sony to immediately identify the Data Breach, and mitigate the damages at an early stage. The computer system and network alarms were either not in place, not taken seriously, or completely ignored. Actively monitoring logs, including event logs, syslogs, web server logs, firewall logs, anti-virus logs and logging of the various computer systems and networks running in the organization would have saved the day for Sony and allowed it to sound the alarm before it was too late. Various tools exist that allow automation of log monitoring, including systems notifying the system administrator when a data breach is detected. Here, Sony has been left to sift through the logs the hackers left behind in order to identify the source and the real magnitude of the Data Breach.

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

from public WIFI networks.

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

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

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

[6] According to the Ponemon Institute, a data breach costs U.S. companies an average of $201 for each compromised record containing sensitive and confidential PII/PHI – which pegs the estimated cost of the Data Breach to Sony in the multiple millions 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).

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

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

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

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

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

66. Sony flagrantly disregarded and violated Plaintiffs' and Class Members' employment and privacy rights, and harmed them in the process, by failing to accurately and completely notify and inform them about the Data Breach and the disclosure of their PII/PHI.

67. Sony's inadequate Data Breach notification – including its failure to provide Plaintiffs and Class Members with adequate and reasonable protection or sufficient relief from

the Data Breach – substantially increased Plaintiffs' and Class Members' imminent risk of identity theft, identity fraud or medical fraud.

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

69. According to the FTC, the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and any privacy framework should recognize additional harms that might arise from unanticipated uses of data.[8] Further, according to the FTC, there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII. *Id*.

70. According to Javelin Strategy & Research's 2012 Identity Fraud Report (the "Javelin Report"), as recently as 2011, the mean consumer cost of rectifying identity fraud was $354 while the mean resolution time of identity fraud was 12 hours. *Id.* at 6. In 2011, the consumer cost for new account fraud and existing non-card fraud increased 33% and 50% respectively. *Id.* at 9. Consumers who received a data breach notification had a fraud incidence rate of 19% in 2011 and, of those experiencing fraud, 43% reported their credit card numbers were stolen and 22% of the victims reported their debit card numbers were stolen. *Id.* at 10. More important, consumers who were notified that their PII/PHI had been breached

---

[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.*

[8] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: 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).

were 9.5 times more likely to experience identity fraud than consumers who did not receive such a notification. *Id.* at 39.

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

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

73. A person whose personal information has been compromised may experience identity fraud for *years*. According to the GAO's June 2007 report on Data Breaches:

> [O]nce stolen data have been sold or posted on the Web, fraudulent use of that 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.

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

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

75. "[H]ealth information is far more valuable than Social Security numbers" on the cyber black market, according to Dr. Deborah Peel, founder and chairwoman of Patient

[9] *See* http://www.stopthehacker.com/2010/03/03/the-underground-credit-card- blackmarket/ (last visited January 2, 2015).

Privacy Rights.[10] An ABC News search uncovered one Internet seller offering medical record database dumps for $14 to $25 per person. *Id.* ABC News was then sent, unsolicited, 40 individuals' private health information, including their names, addresses and body mass index. *Id.* Another inquiry yielded an offer of more than 100 records, including everything from Social Security numbers to persons suffering from anxiety, hypertension, and their HIV status. Plaintiffs' and Class Members' PII/PHI could similarly be valued and traded on the cyber black market. *Id.*

76. Sony flagrantly disregarded and violated Plaintiffs' and Class Members' employment and privacy rights, and harmed them in the process, by depriving them of the value of their PII/PHI, for which there is a well-established national and international market. *See, e.g.*, Soma, *supra* ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted); ABC News Report, *supra*.

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

78. The actual harm and adverse effects to Plaintiffs and Class Members, including the imminent, immediate and continuing increased risk of harm for identity theft, identity fraud or medical fraud directly and proximately caused by Sony's above-described wrongful actions, inaction, omissions, and want of ordinary care, and the resulting Data Breach, requires Plaintiffs and Class Members to take affirmative acts to recover their peace of mind, and personal security – for which there is a financial and temporal cost. Plaintiffs and Class Members have spent significant time and expense engaging in such actions, including, without

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

limitation, (i) identifying and dealing with fraudulent charges, (ii) canceling and securing the reissuance of credit cards and debit cards, (iii) frequently purchasing credit reports from multiple credit reporting agencies, (iv) placing and removing fraud alerts and security freezes on credit reports, (v) purchasing credit monitoring and internet monitoring services, (vi) purchasing identity theft insurance, (vii) reviewing bank statements, credit card statements, and other financial account statements, (viii) closing, modifying and reopening bank accounts and other financial accounts, (ix) dealing with withdrawal and purchase limits imposed on compromised accounts, (x) experiencing the inability to withdraw funds from compromised accounts, (xi) making trips to their financial institutions, (xii) spending time on the telephone attempting to sort out issues related to the Data Breach, (xiii) resetting automatic billing instructions tied to compromised accounts, (xiv) paying late fees and declined payment fees imposed as a result of failed automatic payments, (xv) changing email addresses, or (xvi) updating financial and non-financial accounts with new bank account information, new payment card information, and new email addresses. Plaintiffs and Class Members have suffered, and will continue to suffer, such damages for the foreseeable future.

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

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

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

82. The unauthorized disclosure of a person's Social Security number can be particularly damaging since Social Security numbers cannot be easily replaced like a credit card or debit card. In order to obtain a new Social Security number, a person must show evidence that someone is using the number fraudulently or is being disadvantaged by the misuse. *See Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (December 2013), available at http://www.ssa.gov/pubs/10064.html (last visited January 2, 2015). Thus, a person whose PII/PHI has been compromised cannot obtain a new Social Security number until the damage has already been done.

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

84. Medical identity theft (or medical fraud) occurs when a person's personal information is used without authorization to obtain, or receive payment for, medical treatment, services or goods. For example, according to the most recent census, as of 2010, more than 50

million people in the United States did not have health insurance. This in turn has led to a surge in medical identity theft as a means of fraudulently obtaining medical care. Victims of medical identity theft also may find that their medical records are inaccurate, which can have a serious impact on their ability to obtain proper medical care and insurance benefits.

85. Sony's above-described wrongful actions, inaction, omissions, and want of ordinary care directly and proximately caused the "double Holy Grail of data breaches" – the release, disclosure, and dissemination into the public domain of Plaintiffs' and Class Members' PII/PHI without their knowledge, authorization or consent. As a direct and proximate result of Sony's above-described wrongful actions, inaction, omissions, and want of ordinary care, and the resulting Data Breach, Plaintiffs and Class Members have incurred (and will continue to incur) economic 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), (viii) the imminent, immediate and continuing increased risk of identity theft, identity fraud or medical fraud – for which they are entitled to compensation, and (ix) civil penalties under the PAGA (CAL. LAB. CODE § 2698, *et seq.*).

86. On February 20, 2015, Plaintiff Vargas, through his representative, gave written notice by certified mail to the California Labor and Workforce Development Agency ("LWDA") and to Sony, of the specific provisions of the California Labor Code herein alleged to have been violated, including the facts and legal theories to support the alleged violations. More than 33 days have passed since such notice was given and Plaintiff Vargas has received no indication from the LWDA that it intends to investigate Plaintiff Vargas' allegations. Plaintiff Vargas, therefore, has complied with the administrative prerequisites for bringing a

cause of action on behalf of himself and the other affected current and former employees of Sony pursuant to the PAGA (CAL. LAB. CODE § 2698, *et seq.*).

CLASS ACTION ALLEGATIONS

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

> All current and former Sony employees and independent contractors who are California citizens and 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.

88. Plaintiffs also seek to represent the following sub-classes:

> (A) All current and former Sony employees who are California citizens and 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 Employee Sub-Class"); and
>
> (B) All current and former Sony independent contractors who are California citizens and 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").

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

90. Excluded from the Class and Sub-Classes are the officers, directors, agents and legal representatives of Sony, and any entity in which Sony or any Sony subsidiary has a controlling interest, and the Court and Court personnel.

91. The Class Members are so numerous that their joinder is impracticable. According to information disclosed by Sony in the media, there are over 47,000 Class Members. More than two-thirds (*i.e.*, 100%) of the members of the proposed class are

California citizens. The precise number, identity, and contact information of each Class Member is currently unknown to Plaintiffs, but can be easily derived from the internal records Sony used to send the Data Breach Notification Letters to Plaintiffs and Class Members.

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

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

(i) Whether Sony adequately designed, adopted, implemented, controlled, directed, oversaw, managed, monitored and audited the appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class Members' PII/PHI that was disclosed without authorization in the Data Breach;

(ii) Whether Sony's failure to properly safeguard and protect Plaintiffs' and Class Members' PII/PHI was willful, reckless, arbitrary, capricious and otherwise not in accordance with applicable protocols, procedures, guidelines, laws and regulations;

(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 disclosure of Plaintiffs' and Class Members' PII/PHI violated the California CMIA (CAL. CIV. CODE § 56, *et seq*.);

(v) Whether 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 violated the California Unfair Competition Law (CAL. BUS. & PROF. CODE § 17200, *et seq*.);

(vi) Whether 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 violated the California Security Requirements for Consumer Records (CAL. CIV. CODE §§ 1798.29 and 1798.80, et. *seq*.);

(vii) Whether 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 violated Article 1, § 1 of the California Constitution;

(viii) Whether 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 constitutes negligence at California common law;

(ix) Whether 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 constitutes invasion of privacy by public disclosure of private facts at California common law;

(x) Whether 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 constitutes unjust enrichment/assumpsit at California common law;

(xi) Whether Plaintiffs and Class Members suffered harm or injury 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;

(xii) 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;

(xiii) 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;

(xiv) 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; and

(xv) Whether Plaintiff Vargas and Sony Employee Sub-Class Members are entitled to representation under the Private Attorneys General Act of 2004, CAL. LAB. CODE § 2698, *et seq.*, and recovery of the corresponding civil penalties as a direct and/or proximate result of Sony's wrongful actions, inaction, omissions, and/or want of ordinary care that directly and/or proximately caused the Data Breach and the unauthorized disclosure of Plaintiffs' and Sony Employee Sub-Class Members' PII/PHI.

94. Plaintiffs' claims are typical of the claims of the Class Members because Plaintiffs, like all Class Members, are victims of Sony's wrongful actions, inaction, and

omissions, and want of ordinary care that directly and proximately caused the Data Breach, caused the unauthorized disclosure of Plaintiffs' and Class Members' PII/PHI, and caused Plaintiffs and Class Members to suffer the resulting economic damages, injury and harm.

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

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

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

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

99. Certification of the Class also is appropriate because the prosecution of separate actions by individual Class Members would create a risk of establishing incompatible standards of conduct for Sony. For example, one court might decide the challenged wrongful

actions, inaction, omissions, and want of ordinary care are illegal and enjoin Sony, while another court might decide that the same wrongful actions, inaction, omissions, and want of ordinary care are not illegal. Individual actions also could be dispositive of the interests of the other Class Members who were not parties to such actions and substantially impair or impede their ability to protect their interests.

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

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

102. Absent a class action, Sony will retain the benefits of its wrongdoing despite its serious violations of the law and infliction of economic damages, injury and actual harm on 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 and Sub-Class Member)

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

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

105. At all relevant times, Sony was both a contractor and a health care provider because it had the "purpose of maintaining medical information . . . in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage his

or her information, or for the diagnosis or treatment of the individual." CAL. CIV. CODE § 56.06(a).

106. At all relevant times, Sony collected, stored, managed, and transmitted Plaintiffs' and Class Members' PII/PHI.

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

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

109. Sony also violated Sections 56.06 and 56.101 of the California CMIA, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction or disposal of confidential PHI. 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, Plaintiffs' and Class Members' confidential PHI was wrongfully released and disclosed without their authorization.

110. 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, and violation of the CMIA, 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 or medical fraud – for which they are entitled to compensation.

111. 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 and its violation of the CMIA, Plaintiffs and Class Members also are entitled to (i) injunctive relief, (ii) punitive damages of up to $3000 per Plaintiffs and each Class Member, and (iii) attorneys' fees, litigation expenses and court costs under CAL. CIV. CODE § 56.35.

COUNT II

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW

(CAL. BUS. & PROF. CODE § 17200, *et seq.*)

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

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

113. The California Unfair Competition Law, CAL. BUS. & PROF. CODE § 17200, *et seq*. ("UCL"), prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as those terms are defined by the UCL and relevant case law. By virtue of its above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Sony engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the UCL.

114. In the course of conducting its business, Sony committed "unlawful" business practices by, *inter alia*, knowingly failing to 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 – even after suffering at least one recent widespread corporate data breach – violating the statutory and common law alleged herein in the process, including, *inter alia*, the California CMIA, the California Security Requirements for Consumer Records Act, and Cal. Lab. Code §§ 2698, 2800 and 2802. Plaintiffs and Class Members reserve the right to allege other violations of law by Sony constituting other unlawful business acts or practices. Sony's above-described wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

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

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

117. The UCL also prohibits any "fraudulent business act or practice." Sony's above-described claims, nondisclosures and misleading statements were false, misleading and likely to deceive the consuming public in violation of the UCL.

118. 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 and its violations of the UCL, 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 or medical fraud – for which they are entitled to compensation.

119. As part of its corporate culture, Sony has taken – and touted – a cavalier attitude towards safeguarding and protecting PII/PHI in its possession, custody, and control and a cavalier attitude towards cyber security. As a result, Sony has released and disclosed sensitive and confidential PII and PHI entrusted to it on multiple prior occasions. Unless restrained and enjoined, Sony will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of themselves, Class Members, and the general public, also seek restitution and an injunction prohibiting Sony from continuing such wrongful conduct, and requiring Sony to modify its corporate culture 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 the PII/PHI entrusted to it, as well as all other relief the Court deems appropriate, consistent with CAL. BUS. & PROF. CODE § 17203.

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 and Sub-Class Member)

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

121. 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.

122. 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.

123. By its above-described wrongful actions, inaction, omissions, and want of ordinary care, Sony failed to 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.

124. 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.

125. 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.

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

127. 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 and its violations of CAL. CIV. CODE §§ 1798.29 and 1798.82, 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 or medical fraud – for which they are entitled to compensation.

COUNT IV

INVASION OF PRIVACY BY PUBLIC DISCLOSURE OF PRIVATE FACTS

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

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

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

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

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

132. Sony intentionally invaded Plaintiffs' and Class Members' privacy by repeatedly failing and refusing to 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.

133. Sony's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach constituted (and continue

to constitute) an invasion of Plaintiffs' and Class Members' privacy by publicly disclosing their private facts (*i.e.*, their PII/PHI) without authorization at California common law.

134. 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, or medical fraud – for which they are entitled to compensation.

COUNT V

CONSTITUTIONAL INVASION OF PRIVACY

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

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

136. Article 1, § 1 of the California Constitution provides that "[a]ll people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

137. Plaintiffs and Class Members had (and continue to have) a legally protected privacy interest in the PII/PHI they provided to Sony that Sony released and disseminated without their authorization.

138. Plaintiffs and Class Members also had (and continue to have) a reasonable expectation of privacy regarding such PII/PHI under the circumstances.

139. Sony's above-described wrongful actions, inaction, omissions, and want of ordinary care, and unauthorized release and disclosure of Plaintiffs' and Class Members' PII/PHI constitute a serious invasion of their protected privacy interests in such PII/PHI in violation of Article 1, § 1 of the California Constitution.

140. 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 or medical fraud – for which they are entitled to compensation.

COUNT VI

NEGLIGENCE/GROSS NEGLIGENCE/NEGLIGENCE *PER SE*

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

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

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

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

144. Sony also had (and continues to have) a duty to establish and foster a corporate culture that supports safeguarding and protecting PII/PHI within its possession, custody, and

control, 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 the PII/PHI entrusted to it – including Plaintiffs' and Class Members' PII/PHI.

145. Sony's duties arise from, *inter alia*, CAL. CIV. CODE § 56, *et seq*., CAL. BUS. & PROF. CODE § 17200, *et seq*., and CAL. CIV. CODE §§ 1798.29 and 1798.80, *et seq*.

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

147. Sony violated these standards and duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII/PHI by failing to 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 PII/PHI entrusted to it – including Plaintiffs' and Class Members' PII/PHI.

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

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

150. Sony, by and through its above negligent or grossly negligent actions, inaction, omissions, and want of ordinary care, further breached its duties to Plaintiffs and Class Members by failing to design, adopt, implement, control, direct, oversee, manage, monitor and

audit its processes, controls, policies, procedures, protocols, and software and hardware systems for complying with the applicable laws and safeguarding and protecting their PII/PHI.

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

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

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

154. 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, or medical fraud – for which they are entitled to compensation.

COUNT VII

BREACH OF CONFIDENTIALITY

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

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

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

157. 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.

158. 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.

159. 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.

COUNT VIII

INDEMNIFICATION

(CAL. LAB. CODE §§ 2800 and 2802)

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

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

161. 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.

162. 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.

163. 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 Sony's unauthorized release, disclosure, and dissemination of their PII/PHI to the world.

164. 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

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.

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

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

COUNT IX

UNJUST ENRICHMENT/ASSUMPSIT

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

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

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

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

COUNT X

REPRESENTATION UNDER THE PRIVATE ATTORNEYS GENERAL ACT OF 2004 AND THE IMPOSITION OF CIVIL PENALTIES (CAL. LAB. CODE § 2698, *et seq.*)

(On Behalf of Plaintiff Hiram A. Vargas and Each Aggrieved Sony Employee)

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

171. In addition to, or in the alternative, Plaintiff Vargas, as an "aggrieved employee," brings this action as a representative action on behalf of himself and all other current and former Sony employees under the California Private Attorneys General Act of 2004, CAL. LAB. CODE § 2698, *et seq.* ("PAGA"). In particular, Plaintiff Vargas seeks to recover civil penalties under PAGA, including CAL. LAB. CODE § 2699, for Sony's violations of the California Labor Code alleged above.

172. Among other things, and without limitation, CAL. LAB. CODE § 2699.5 provides that aggrieved current or former employees--such as Plaintiff Vargas--may maintain a representative action for civil penalties against Sony for its following above-described wrongful conduct:

(i) Sony's failure to indemnify its current and former employees for losses directly and/or proximately caused by Sony's above-described want of ordinary care (CAL. LAB. CODE § 2800); and

(ii) Sony's failure to indemnify current and former employees for all necessary losses and expenses incurred in directly discharging their duties as Sony employees (CAL. LAB. CODE § 2802).

173. Under CAL. LAB. CODE § 2699(f)(2), therefore, Plaintiff Vargas, on behalf of himself and Sony Employee Sub-Class Members, seeks to recover civil penalties under PAGA in the amount of "one hundred dollars ($100) for each aggrieved employee per pay period for the initial violation and two hundred dollars ($200) for each aggrieved employee per pay period for each subsequent violation."

RELIEF REQUESTED

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

175. **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), (viii) the imminent, immediate and continuing increased risk of identity theft, identity fraud or medical fraud – for which they are entitled to compensation, and (ix) civil penalties under the PAGA (CAL. LAB. CODE § 2698, *et seq.*). 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.

176. **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.

177. **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 wrongful conduct including, without limitation, the unauthorized release and disclosure of its current and former employees' and independent contractors' PII/PHI, (v) requiring Sony to modify its corporate culture 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 the PII/PHI entrusted to it, (vi) periodic compliance audits by a third party to insure that Sony is properly safeguarding and protecting the PII/PHI in its possession, custody, and control, and (vii) clear and effective notice to Class Members about the serious risks posed by the theft of the PII/PHI and the precise steps that must be taken to protect themselves.

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

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

(i) actual, incidental, consequential, and nominal damages to be determined by the trier of fact;

(ii) statutory damages (as set forth above);

(iii) civil penalties (as set forth above);

(iv) punitive damages (as set forth above);

(v) equitable relief, including restitution, disgorgement of all amounts by which Sony has been unjustly enriched (as set forth above);

(vi) pre- and post-judgment interest at the highest legal rates applicable;

(vii) appropriate injunctive relief (as set forth above);

(viii) attorneys' fees and litigation expenses;

(ix) costs of suit; and

(x) 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.

Respectfully Submitted,

Dated: May 6, 2015

BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
THOMAS J. O'REARDON II (247952)
PAULA M. ROACH (254142)

By: Timothy Blood /pr
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
proach@bholaw.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

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

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 Bruce Ochmanek, Hiram A. Vargas, and the Putative Class

JOHNSON & JOHNSON LLP
DOUGLAS L. JOHNSON (209216)
NEVILLE L. JOHNSON (66329)
BRIAN T. SHIPPEN-MURRAY (288188)
439 North Canon Drive, Suite 200
Beverly Hills, CA 90210
djohnson@jjllplaw.com
njohnson@jjllplaw.com
bmurray@jjllplaw.com

Attorneys for Plaintiffs Susan Dukow, Sherrill Perryman,and the Putative Class

RIDOUT LYON + OTTOSON LLP
CHRISTPHER P. RIDOUT (143931)
CALEB MARKER (269721)
HANNAH P. BELKNAP (294155)
555 E. Ocean Blvd., Suite 500
Long Beach, CA 90802
c.ridout@rlollp.com
c.marker@rlollp.com
h.belknap@rlollp.com

LOWE & ASSOCIATES PC
STEVEN T. LOWE (122208)
KRIS S. LE FAN (278611)
KATRINA V. NOVAK (290229)
11400 W. Olympic Blvd., Suite 640
Los Angeles, CA 90064
steven@lowelaw.com
kris@lowelaw.com
katrina@lowelaw.com

Attorneys for Plaintiff L. Churchill, and the Putative Class

NICHOLAS & TOMASEVIC LLP
CRAIG M. NICHOLAS (178444)
ALEX M. TOMASEVIC (245598)
MEI-YING M. IMANAKA (280472)

225 Broadway, 19th Floor
San Diego, CA 92101
cnicholas@nicholaslaw.org
atomasevic@nicholaslaw.org
mimanaka@nicholaslaw.org

COLEMAN FROST LLP
DERRICK F. COLEMAN (170955)
R. JEFFREY NEER)10-418_
429 Santa Monica Blvd., #700
Santa Monica, CA 90401
derrick@colemanfrost.com
jeff@colemanfrost.com

Attorneys for Plaintiff Amy McKenzie and the Putative Class

DECLARATION OF SERVICE

Susan Dukow, et al. v. Sony Pictures Entertainment, Inc.
Los Angeles Superior Court Case No. BC566884

I, the undersigned, declare:

1. That declarant is and was, at all times herein mentioned, a citizen of the United States and a resident of the State of California, over the age of 18 years, and not a party to or interested party in the within action; that declarant's business address is 701 B Street, Suite 1700, San Diego, California 92101.

2. That on May 6, 2015, declarant caused to be served the foregoing document upon the attorney of record for each party in this case at the e-mail address(es) registered for such service via electronic transmission to File & Serve*Xpress* at fileandservexpress.com.

3. That on May 6, 2015, declarant caused to be served the foregoing document upon any non-registered participants via electronic transmission as follows:

I declare under penalty of perjury that the foregoing is true and correct. Executed on May 6, 2015.

Janet Kohnenberger
BLOOD HURST & O'REARDON, LLP
701 B Street, Suite 1700
San Diego, CA 92101
Telephone: (619) 338-1100
Facsimile: (619) 338-1101
jkohnenberger@bholaw.com

Attachment (Exhibit A) to
Consolidated Amended Complaint

SONY
PICTURES

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.