Raúl Pérez (SBN 174687)
Raul.Perez@Capstonelawyers.com
Jordan L. Lurie (SBN 130013)
Jordan.Lurie@capstonelawyers.com
Robert Friedl (SBN 134947)
Robert.Friedl@capstonelawyers.com
Tarek H. Zohdy (SBN 247775)
Tarek.Zohdy@capstonelawyers.com
Cody R. Padgett (SBN 275553)
Cody.Padgett@capstonelawyers.com
Capstone Law APC
1840 Century Park East, Suite 450
Los Angeles, California 90067
Telephone: (310) 556-4811
Facsimile: (310) 943-0396

Attorneys for Plaintiff Marcela Bailey

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

MARCELA BAILEY, individually, and on behalf of a class of similarly situated individuals,

Plaintiff,

v.

SONY PICTURES ENTERTAINMENT INC,, a Delaware corporation,

Defendant.

Case No.: 2:14-cv-9755

CLASS ACTION COMPLAINT FOR:

(1) Violations of Cal. Civ. Code § 1798.80, *et seq.* (California Security Breach Notification Act);
(2) Negligence;
(3) Violations of Cal. Civ. Code § 56, *et seq.* (California Confidentiality of Medical Information Act);
(4) Violations of 15 U.S.C. §1681w; 16 C.F.R. § 682, *et seq.* (Fair Credit and Reporting Act and Fair and Accurate Credit Transactions Act);
(5) Negligent Hiring; and
(6) Violations of California Business & Professions Code § 17200, *et seq.* (Unfair Competition Law)

DEMAND FOR JURY TRIAL

INTRODUCTION

1. This action involves a multi-billion dollar conglomerate that failed to take the necessary steps to protect the confidential information of its employees, and then left these employees and their family members to fend for themselves in responding to the crisis. Plaintiff Marcela Bailey ("Plaintiff") brings this action for herself and on behalf of all others similarly situated, upon personal knowledge of the facts pertaining to them and on information and belief as to all other matters against Sony Pictures Entertainment Inc. ("Sony Pictures," or "Defendant"). Plaintiff, who had her personal identifiable information ("PII") accessed, stolen, and used without her authorization due to a wide-spread data breach into Sony Pictures' network and servers, alleges that, because of the negligence, breaches of statutory law, and other acts and omissions described herein on the part of Sony Pictures, she suffered actual harm and monetary damages. The harm suffered by Plaintiff extended to her immediate family, as her husband's and children's confidential information was also accessed, stolen and used without authorization.

2. On or about November 24, 2014, hackers calling themselves "Guardians of Peace" (or "#GOP") seized control of Sony Pictures' internal network, bringing the company's operations to a grinding halt.[1] As Sony Pictures scrambled to get its network, including its email, servers, and other internal systems back online, several executives received threat of extortion to themselves and their families, demanding that Defendant cease the release of the upcoming comedy, "The Interview," which depicts a fictional assassination attempt on North Korea's leader Kim Jung Un.[2]

[1] *See* Los Angeles Times, "Sony Pictures returning to normal after crippling computer attack," http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-hacking-20141202-story.html (last visited Dec. 17, 2014).

[2] *See* Ars Technica, "Sony Pictures attackers demand: 'Stop the terrorist

3. On or about November 29, 2014, #GOP dropped the first of many bombs—five new Sony Pictures movies were discovered to be heavily traded online.[3] But that was just the tip of the iceberg. In early December, with Sony Pictures standing on the sidelines doing little to safeguard the confidential information of its employees, hackers publicly released highly sensitive, personal information regarding former and current employees obtained from Sony Pictures' networks and servers, which were insufficiently secured, poorly protected, or non-encrypted, including names, addresses, phone numbers, birthdates, Social Security Numbers ("SSNs"), email addresses, criminal background checks, salary and job details, termination letters, accounting and routing numbers associated with employee names, and health insurance reimbursements and appeals forms.[4] Since then, the hackers have continued to leak a plethora of Sony Pictures' intellectual property such as files for unreleased and new movies, trade secrets and business models such as movie budgets, executive salary information, and confidential communications and documents regarding personnel or human resource matters.

4. Sony Pictures is no stranger to such attacks. It had previously been the subject of data breach attacks in the past, including the Sony PlayStation data breach in April of 2011, which exposed the personal information of 77 million

---

film!'" http://arstechnica.com/security/2014/12/sony-pictures-attackers-demand-stop-the-terrorist-film/ (last visited Dec. 17, 2014).

[3] *See* Hollywood Reporter, "Several Sony Films Leak Online After Hack Attack," http://www.hollywoodreporter.com/news/sony-films-leak-online-hack-752821 (last visited Dec. 17, 2014).

[4] *See* CSO Online, "The breach at Sony Pictures is no longer just an IT issue," http://www.csoonline.com/article/2854672/business-continuity/the-breach-at-sony-pictures-is-no-longer-just-an-it-issue.html (last visited Dec. 17, 2014). *See also* BuzzFeed News, "Sony Could Face Class Action Lawsuit For Data Breach," http://www.buzzfeed.com/matthewzeitlin/sony-could-face-class-action-lawsuit-for-data-breach (last visited Dec. 17, 2014).

user accounts[5] and a subsequent breach of Sony Pictures Entertainment websites in June of 2011, which leaked 1 million individuals' personal information.[6] More recently, Sony Pictures' systems in Germany and Brazil were also subjected to malicious activity by hackers. Notwithstanding these repeated attacks, Sony Pictures and other Sony companies remain non- or sub-par compliant with industry standards. As a result of this negligence and indifference, once again, extremely sensitive data, which Sony Pictures had a duty to protect, has been released.

5. Plaintiff brings this case as a class action on behalf of herself and the more than 47,000 current and former employees, contractors, and freelancers who have had their personal identifiable, health, medical, personnel, and human resources, and financial information accessed without their authorization and used illegally as a result of Defendant's acts and failures to act.

6. Sony Pictures caused personal identifying and financial information about Plaintiff and the Class to be accessed, collected, downloaded, saved, distributed, transferred, and used by various individuals and entities without knowledge or consent of Plaintiff and the Class. Sony Pictures also failed to timely and reasonably notify Plaintiff and the Class of such unauthorized access and breach of their privacy interests, notice which is explicitly required by the laws of California. A whole three weeks after announcement of the data breach, Sony Pictures still has not provided notice to former employees regarding the security breach. Instead, Sony Pictures has left Plaintiff and formerly employed class members in the dark on the situation while they scramble to take steps of

[5] *See* Reuters, "Sony PlayStation suffers massive data breach," http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426 (last visited Dec. 17, 2014).

[6] *See* Mashable, "Sony Pictures Website Hacked, 1 Million Accounts Exposed," http://mashable.com/2011/06/02/sony-pictures-hacked/ (last visited Dec. 17, 2014).

their own to protect their identities and credit, and that of any affected family members.

7. Although the full extent of the sensitive information leaked remains to be seen, CSOOnline[7] and Wired.com[8] revealed that the breached network contained the following types of PII, as defined in California Civil Code sections 1798.80 and 1798.82:[9]

a. Names,
b. Social Security Numbers,
c. Phone numbers (including unlisted phone numbers),
d. Home addresses,
e. Birth dates,
f. Financial account information (including banking, credit card, and other financial account numbers);
g. Other sensitive data collected and maintained by Sony Pictures and its human resource departments, including financial, medical, and health insurance information.

[7] *See* CSO Online, "The breach at Sony Pictures is no longer just an IT issue," http://www.csoonline.com/article/2854672/business-continuity/the-breach-at-sony-pictures-is-no-longer-just-an-it-issue.html (last visited Dec. 17, 2014).

[8] *See* Wired.com, "Sony Got Hacked Hard: What We Know and Don't Know So Far," http://www.wired.com/2014/12/sony-hack-what-we-know/ (last visited: December 15, 2014).

[9] Cal. Civ. Code section 1798.80 defines "personal information" (e) "Personal information" means any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.

Cal. Civ. Code section 1798.82 defines "personal information" (1) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (A) Social security number. (B) Driver's license number or California identification card number. (C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (D) Medical information. (E) Health insurance information. (2) A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

8. Additionally, upon information and belief, other personal, sensitive information that was among the stolen data also included:

a. Email addresses;
b. Employment information, such as human resources' performance reviews, salaries, and bonus information.
c. Criminal background checks and termination records;
d. Correspondence about employee medical conditions; and
e. Internal email spools.

9. Plaintiff believes and alleges that Sony Pictures failed to securely store or properly maintain this sensitive and confidential employee PII, with encryption or password protection to secure it, to any degree, from unauthorized access and/or theft.

10. Despite the fact that this stunning leak of extraordinary amounts of individuals' PII might have been set into motion a year ago, on information and belief, Sony Pictures deliberately delayed in notifying Plaintiff and other class members of the breach. Had Sony Pictures provided prompt notice of the breach in accordance with the data breach notification laws of California, Plaintiff and the Class could have and would have taken steps to protect themselves sooner, including, but not limited to, monitoring their identities and credit from theft.

11. Instead, for reasons unknown to Plaintiff and the Class, but unrelated to law enforcement requirements, Sony Pictures recklessly chose to delay until December 8, 2014, to officially notify only current employees about the devastating and widespread breach. Conspicuously absent was any formal notice to the hundreds of former employees. On or about December 15, 2014, Sony Pictures posted another notification letter on its website (http://www.sonypictures.com) titled "Message for current and former Sony Pictures employees and dependents, and for production employees." Sony Pictures, however, has yet to send a formal notice about the incident to its former employees, including Plaintiff, who are class members.

12. Such deliberate and/or grossly negligent conduct, in the face of a

breach that was avoidable had Defendant taken appropriate steps to secure Plaintiff's and the Class's PII, is actionable under the statutes and common law of the United States and California, where members of the Class reside.

13. This lawsuit seeks to remedy the detrimental effects of the breach of Plaintiff's and class members' privacy interests, the failure to timely and reasonably notify Plaintiff and the Class of the breach in accordance with California law, the failure to abide by other laws that required their PII be secured or disposed of properly, the misleading and deceptive notification letter from Sony Pictures dated December 8, 2014, a subsequent notification later posted to Sony Pictures' website (http://www.sonypictures.com/) dated December 15, 2014, and the insufficient remedy offered by Defendant.

JURISDICTION AND VENUE

14. Plaintiff alleges that Defendant was incorporated in the State of Delaware. Plaintiff is a resident and citizen of California. Plaintiff and other members of the Class are citizens of states different from Defendant. Plaintiff alleges on information and belief that the total amount in controversy related to her claims is in excess of $75,000. Thus, this Court has original jurisdiction over this action pursuant to 28 U.S.C. § 1332(a). Moreover, Plaintiff alleges, on information and belief, that the aggregate amount in controversy for this class action exceeds five million dollars ($5,000,000.00), exclusive of interest and costs, and that the class exceeds 100 members, pursuant to 28 U.S.C. § 1332(d).

15. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a), (b) and (d) because Defendant maintains offices, has agents, and is licensed to transact and does transact business throughout this district and because a substantial part of the events or omissions giving rise to the claims occurred within this District.

THE PARTIES

Plaintiff

16. Plaintiff Marcela Bailey is a California citizen who resides in Los Angeles, California. Plaintiff was employed by Sony Pictures for approximately 20 years from January 1991 to February 2013. Plaintiff's PII was stored on Sony Pictures' network of servers on or before November 2014 and was compromised as part of the recent data breach.

17. On November 24, 2014, Plaintiff received three automated pre-recorded calls from Sony Picture's emergency notification line throughout the day. Although Plaintiff is a former employee, she nevertheless received these calls because Sony Pictures had not removed Plaintiff from its employee emergency notification list. The recordings, which were presumably made to all current Sony Pictures employees, only instructed Sony Pictures employees to shut down their computers and log off until further notice. Upon hearing the recording, Plaintiff emailed Sony Pictures requesting that she be removed from their emergency employee notification list as she was no longer an employee. After Plaintiff's email bounced back as non-deliverable, Plaintiff contacted a member of Sony responsible for overseeing the emergency phone system asking to be removed from the call list. Plaintiff received a response that evening stating that she would be removed and stating that there was a major hack, but no mention was made that her PII had been or was in danger of being disclosed.

18. Throughout the evening, Plaintiff also had heard various breaking news reports regarding the security breach at Sony Pictures. Obviously concerned given her prior employment with Defendant, Plaintiff closely followed the developing stories and news coverage regarding the security breach since the day the attack was made public. Once it became clear that the security breach involved the unauthorized access to and public disclosure of former employees' PII, Plaintiff became very concerned about the risk of identity theft

and disclosure of extremely private and sensitive information that was contained in her personnel file with Sony Pictures, along with private and confidential information pertaining to her family

19. Since the subject data breach, Plaintiff has expended significant time, effort, and incurred expenses in order to protect her and her family's PII from being used or attempted to be used by unknown third parties to access, use, or alter Plaintiff and her family's bank and credit accounts and other PII. For example, Plaintiff has closely monitored news coverage and reports pertaining to the breach each day since she first learned of the breach. Plaintiff has also spent considerable time monitoring her and her family's bank accounts for suspicious activity and contacting financial institutions to place credit freezes. Given Sony's failure to provide sufficient notice and updates, Plaintiff has already had to spend 30 to 40 hours reading developing stories and news coverage regarding the data breach to keep herself apprised of the situation for her and her family's protection.

20. In addition, Plaintiff has spent time reaching out to Sony Pictures to try to obtain more information regarding the scope of the breach and information on how Sony Pictures might mitigate the imminent risk of harm to former employees. After Plaintiff did not hear from Sony Pictures regarding any plan to mitigate the risk of identity theft and/or unauthorized credit use to former employees, Plaintiff purchased LifeLock identity theft protection for herself, her husband, and her three children. The cost of Lifelock's identity theft protection services to Plaintiff is $1028.05 annually. This is an expense that Plaintiff was forced to incur directly as a result of Sony Picture's failure to safeguard her PII and utter indifference in helping her family mitigate the data breach harm.

21. As of the date of this complaint, Plaintiff still has not received notice from Sony Pictures regarding the theft of her PII. Similarly, Plaintiff's husband, himself a former employee of Sony Pictures, and her three then-

dependents also have not received notice from Sony Pictures regarding the security breach.

Defendant

22. Defendant Sony Pictures Entertainment Inc. (hereinafter "Defendant" or "Sony Pictures") is a corporation organized and in existence under the laws of the State of Delaware and registered to do business in the State of California. Defendant's Corporate Headquarters are located at 10202 W. Washington Blvd., Culver City, CA 90232. Defendant employed or previously employed prospective class members at the time of the data breach.

23. Defendant is a subsidiary of Tokyo-based Sony Corporation. Defendant's corporate offices and production facilities are headquartered in Culver City, California, where it owns and operates a studio facility, Sony Pictures Studios. Defendant Sony Pictures is comprised of Sony's motion picture and television production and distribution units, and the aggregate results of its worldwide operations for the second fiscal quarter, ending September 30, 2014, are reported to be $1.671 billion.

FACTUAL BACKGROUND

24. Despite numerous warning signs, Sony Pictures failed to adhere to standard business practices for protecting employee PII. This failure has left Plaintiff, class members, and their dependents whose information was also exposed, unprotected and at a heightened risk for identity theft.

Guidance and Standard Business Practices for Protecting Employee PII

25. Companies often keep in their files stores of sensitive information. including names, Social Security information, credit card data, and health or medical information regarding their employees. This information is often utilized to perform basic business functions, such as paying employees, and payroll.

26. However, in recent years, due to the proliferation of massive-scale

data breaches and the sheer amount of PII that can be accumulated (and thereby put at risk) by companies, federal and state legislatures passed numerous laws to ensure that companies protect the security and confidentiality of sensitive PII in their files. These laws impose obligations on companies to proactively maintain reasonable security measures to protect the PII of individuals. For example, 16 C.F.R. § 682.3(a) of the Fair and Accurate Credit Transactions Act ("FACTA") requires employers to properly dispose of consumer report information. Other laws impose requirements on employers to establish training procedures for its agents handling files and restricted access security systems to protect sensitive medical information, such as the California Confidentiality of Medical Information Act (codified in Cal. Civ. Code § 56 *et seq.*).

27. Additionally, the Federal Trade Commission ("FTC") has issued publications regarding recommended business practices for securing PII, e.g. "Protecting Personal Information: A Guide for Business" (updated Nov. 2011).[10] This FTC publication provides guidelines for businesses to develop a "sound data security plan" to protect against security breaches and identity theft. In order to protect sensitive, personally identifying information in company files, the report instructs businesses to follow basic guidelines such as encrypting PII and limiting the collection and storage of PII, like SSNs, for legitimate business needs, and only for as long as necessary. Additional guidelines include controlling access to sensitive information by requiring that employees use "strong" passwords that are longer and frequently changed, and inventorying all equipment that stores PII or connects to computers where PII is stored, such as computers, mobile or wireless devices like smartphones, flash drives, and digital copiers. The FTC also recommends that businesses implement disposal practices

[10] *See* Federal Trade Commission, ""Protecting Personal Information: A Guide for Business." Available at http://www.business.ftc.gov/documents/bus69-protecting-personal-information-guide-business; last visited Dec. 18, 2014.

for physically and digitally stored information that are reasonable and appropriate to prevent unauthorized access to or use of personally identifying information.

28. The California Department of Justice, Office of the Attorney General, Privacy Enforcement and Protection Unit, also published a similar set of guidelines in its January 2012 report. The report, "Recommendation Practices of Notice of Security Breach Involving Personal Information," suggests best practices guidance similar to those in the FTC publication.[11] The California report also suggests rules and criteria building on the federal guidelines, e.g., a recommendation for businesses to utilize data encryption, in combination with host protection and access control, to protect higher risk PII whenever feasible.

29. On information and belief, Sony Pictures blatantly failed to follow many of these basic guidelines. For example, Sony Pictures stored thousands of passwords in a very obviously named file called "**Password**." Furthermore, Defendant used plaintext and unencrypted Word documents and Excel spreadsheets to save usernames and passwords to Sony Pictures' internal computers, social media accounts, and web service accounts.[12]

30. Furthermore, Sony Corporation failed to develop proper reporting procedures after oversight of the monitoring of Sony subsidiaries was transferred from a third-party security vendor to its Global Security Incident Response Team ("GSIRT"), an internal group of only 11 employees.[13] Thus, according to a

[11] Available at the State of California, Department of Justice, Office of the Attorney General's website: http://oag.ca.gov/privacy/business-privacy.

[12] *See* Network World, "Sony hacked in February, knew about security flaws before data leak," http://www.networkworld.com/article/2859473/microsoft-subnet/sony-hacked-in-feb-knew-about-huge-security-flaws-before-cybersecurity-train-wreck.html (last visited Dec. 17, 2014).

[13] *See* Fusion.net, "Sony Pictures Hack Was a Long Time Coming, Say Former Employees," http://fusion.net/story/31469/sony-pictures-hack-was-a-long-time-coming-say-former-employees/ (last visited Dec. 17, 2014).

scathing September 2014 internal information technology ("IT") assessment, by 2013, a significant number of critical security devices in the Sony Pictures network were no longer being monitored, leading the company to be "blind to 17% of their environment." The assessment also warned that "security incidents impacting these network or infrastructure devices may not be detected" or resolved in a timely manner.[14]

31. Everywhere in the news media, many security specialists questioned the data safety precautions used by Sony Pictures, or the lack thereof, to protect employees' and individuals' PII.

32. As described further below, on information and belief, Defendant also failed to heed specific warnings that its network security may have been compromised, and instead chose to turn a blind eye to the numerous red flags. Ultimately, the victims of this massive November 2014 data hack would take the fall for Sony Pictures' negligence.

Proliferation of Use of PII for Identity Theft

33. In a June 2007 report on data breaches, the United States Government Accountability Office ("GAO") found that more than 570 breaches involving theft of personal identifiers such as SSNs were reported by the news media from January 2005 through December 2006.[15] This number only continues to grow. According to a recent nationwide survey, in 2010, 8.1 million Americans were victims of identity theft in 2010.[16]

---

[14] *See* Network World, "Sony hacked in February, knew about security flaws before data leak," http://www.networkworld.com/article/2859473/microsoft-subnet/sony-hacked-in-feb-knew-about-huge-security-flaws-before-cybersecurity-train-wreck.html (last visited Dec. 17, 2014).

[15] U.S. Government Accountability Office, "PERSONAL INFORMATION: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown." Available at http://www.gao.gov/products/GAO-07-737 and last visited Dec. 18, 2014.

[16] State of California, Department of Justice, Office of the Attorney

34. A data breach, where personal information is compromised, can often lead to identity theft. Identity theft occurs when a person's identifying information is used to commit fraud-related crimes such as credit card fraud, phone or utilities fraud, bank fraud, and government fraud. Identity thieves may use identifying data such as SSNs to open financial accounts and incur charges and credit in a victim's name. This type of identity theft may be the "most damaging," because the victim may not become aware of the theft for some time and the victim may incur "substantial costs and inconvenience repairing damage to their credit records . . . [and to their] good name."[17] Leaked SSN information is particularly damaging because identity thieves can also fraudulently access a victim's existing accounts; unfortunately, a stolen SSN cannot be quickly updated and changed like a credit card number. Even updating one's SSN is still not a guarantee of protection against future identity theft.

35. Immediate financial loss is just the tip of the iceberg when identity theft crimes occur, because criminals can often sit on stolen information for years before using and/or selling the personal or financial information to other identity thieves. According to the GAO Report from 2007, "once 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."[18]

36. A nationwide survey estimated the total cost of identity theft in the

---

General, "Recommended Practices on Notice of Security Breach Involving Personal Information," citing Javelin Strategy & Research, 2011 Identity Fraud Survey Report (February 2011), at page 6. Available at http://oag.ca.gov/privacy/business-privacy and last visited Dec. 17, 2014.

[17] U.S. Government Accountability Office, "PERSONAL INFORMATION: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown." Available at http://www.gao.gov/products/GAO-07-737 and last visited Dec. 18, 2014.

[18] *Id.*

U.S. was at $37 billion. The same survey also reported that an average identity theft victim spent $631 and 33 hours to resolve the problem and clear up records.[19]

37. More recently, a particularly pernicious type of identity theft has increased in popularity: medical identity theft, where an individual's name or other identifying information is used to fraudulently obtain medical services or products. Along with the financial ramifications, medical identity theft may also result in dangerously inaccurate information being inserted into the victim's medical records. This form of identity theft can be very difficult to discover and remedy; the established procedures for responding to more-common financial identity theft are not available in the medical realm.[20]

38. To victims, data breaches and ensuing identity theft issues have a very real cost—in time and effort expended, money spent, and the emotional toll taken on an individual. Plaintiff and class members, including dependents whose information was also exposed, must grapple with the ever-present threat of identity theft for the rest of their lifetimes.

Sony Picture's Data Breach Exposed PII of over 47,000 Employees

39. On or about November 24, 2014, hackers calling themselves "Guardians of Peace" (or "#GOP") seized control of Sony Pictures' internal network, bringing the company's operations to a grinding halt.[21] The network

---

[19] State of California, Department of Justice, Office of the Attorney General, "Recommended Practices on Notice of Security Breach Involving Personal Information," citing Javelin Strategy & Research, 2011 Identity Fraud Survey Report (February 2011), at page 6. Available at http://oag.ca.gov/privacy/business-privacy and last visited Dec. 17,

[20] *Id.*, citing research on medical identity theft by the World Privacy Forum, at www.worldprivacyforum.org

[21] *See* Los Angeles Times, "Sony Pictures returning to normal after crippling computer attack," http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-hacking-20141202-story.html (last visited Dec. 17, 2014).

had been hit with destructive "wiper" malware called "Destover" or "Wipall," which reportedly infected and erased hard drives at the movie studio.[22]

40. As Sony Pictures scrambled to get its network back online, including its email, servers, and other internal systems, several executives received threat to themselves and their families, demanding that Defendant cease the release of the upcoming comedy, "The Interview," which depicts a fictional assassination attempt on North Korea's leader Kim Jung Un.[23] After the hackers took control of corporate systems, the #GOP cyber attackers began leaving behind intimidating blackmail messages for Sony workers which appeared when employees attempted to sign onto their computers. The notes warned, "this is just a beginning" and that "[w]e've obtained all of your internal data including your secrets and top secrets. If you don't obey us, we'll release the data shown below to the world."[24]

41. On or about November 29, 2014, #GOP dropped the first of many bombs—five new Sony Pictures movies were discovered to be heavily traded online.[25] Sony Pictures inexcusably seemed more concerned and pre-occupied about this disclosure then the ensuing massive disclosure of employees' confidential information.

42. In early December, hackers publicly released highly sensitive,

---

[22] *See* HealthcareInfoSecurity, "Sony's Breach Notification: The Details," http://www.healthcareinfosecurity.com/sonys-breach-notification-details-a-7682/op-1 (last visited: December 17, 2014).

[23] *See* Ars Technica, "Sony Pictures attackers demand: 'Stop the terrorist film!'" http://arstechnica.com/security/2014/12/sony-pictures-attackers-demand-stop-the-terrorist-film/ (last visited Dec. 17, 2014).

[24] *See* Engadget, "Sony Pictures hack: the whole story," http://www.engadget.com/2014/12/10/sony-pictures-hack-the-whole-story/ (last visited Dec. 18,2014).

[25] *See* Hollywood Reporter, "Several Sony Films Leak Online After Hack Attack," http://www.hollywoodreporter.com/news/sony-films-leak-online-hack-752821 (last visited Dec. 17, 2014).

personal information regarding former and current employees obtained from Sony Pictures' networks and servers, which were insufficiently secured, poorly protected, or non-encrypted, including names, addresses, phone numbers, birthdates, Social Security Numbers ("SSNs"), email addresses, criminal background checks, salary and job details, termination letters, accounting and routing numbers associated with employee names, and health insurance reimbursements and appeals forms.[26]

43. On or about Monday, December 1, 2014, a well-known tech writer for Fusion.net, Kevin Roose, reported that the leak released the salary information of 6,000 Sony Pictures employees.[27] The same day, Sony Pictures issued an internal memorandum to all of its approximately 6,660 current employees, an apparent admission that the large amount of confidential information which was leaked was accurate.[28] On information and belief, no written message was communicated to Plaintiff or other former employees on December 1st. On or about December 2, 2014, Roose reported that he had obtained access to spreadsheets featuring sensitive information about nearly 3,800 Sony Pictures employees, including top executives. The information

[26] *See* CSO Online, "The breach at Sony Pictures is no longer just an IT issue," http://www.csoonline.com/article/2854672/business-continuity/the-breach-at-sony-pictures-is-no-longer-just-an-it-issue.html (last visited Dec. 17, 2014). *See also* BuzzFeed News, "Sony Could Face Class Action Lawsuit For Data Breach," http://www.buzzfeed.com/matthewzeitlin/sony-could-face-class-action-lawsuit-for-data-breach (last visited Dec. 17, 2014).

[27] *See* Fusion.net, "Hacked Documents Reveal a Hollywood Studio's Stunning Gender and Race Gap," http://fusion.net/story/30789/hacked-documents-reveal-a-hollywood-studios-stunning-gender-and-race-gap/ (last visited Dec. 17, 2014).

[28] Hollywood Reporter, "Michael Lynton and Amy Pascal Call Sony Hack "Brazen Attack" In Staff Memo," http://www.hollywoodreporter.com/news/michaellyntonamypascalcall753546 (last visited Dec. 17, 2014).

included employees' birthdates and SSNs.[29]

44. Since then, the hackers have continued to leak a plethora of Sony Pictures' intellectual property such as media files for unreleased and new movies, trade secrets, and business models such as movie budgets, executive salary information, and confidential communications and documents regarding personnel or human resource matters.

45. As Sony Pictures attempted to regain control of the spectacle by instituting damage control regarding the pirated movies and gossip column-worthy email conversations between Hollywood heavy-hitters and Sony Pictures executives, it failed to promptly and adequately address the concerns of one group whose data was now laid bare to the public: **its current and former employees**. As more and more personal, sensitive information was released for the cyber-criminals of the world to download, access, and utilize, Sony Pictures made insufficient attempts to address affected employees' concerns regarding the scope of the breach and how their information would be protected in the future. These employees were treated as a mere afterthought as Sony Pictures was more consumed with protecting its reputation and the image of its top executives as opposed to minimizing the harm to its rank and file.

46. On or about December 8, 2014, a full two weeks after the hackers made their intentions known to Sony Pictures employees, Sony finally sent a notification letter to its employees (this notification letter was also filed with the California Attorney General's office). The letter indicates that the company learned on December 1, 2014, that "the security of personally identifiable information that Sony Pictures received about you and/or your dependents during the course of your employment may have been compromised as a result of [this]

[29] *See* Fusion.net, "More from the Sony Pictures Hack: Budgets, Layoffs, HR scripts, and 3,800 Social Security Numbers," http://fusion.net/story/30850/more-from-the-sony-pictures-hack-budgets-layoffs-hr-scripts-and-3800-social-security-numbers/ (last visited Dec. 17, 2014).

brazen cyber attack." On information and belief, at the time of the filing of this Complaint, Plaintiff and other former employees have not yet received this letter.

47. On or about December 15, 2014, three weeks after the disruption of Sony Pictures' network and systems, Defendant posted another letter on its website (http://www.sonypictures.com) titled "Message for current and former Sony Pictures employees and dependents, and for production employees." This letter, which was never sent to Plaintiff, reiterated some of the basic information from the December 8, 2014 memorandum.

48. On information and belief and as detailed further below, Sony Pictures knew or should have known of the November 2014 breach *at least a year ago*, which is prior to the December 1, 2014, date printed in the above-referenced letters. Sony Pictures also should have reasonably and timely informed employees and other affected individuals about the breach. Instead, Sony Pictures delayed, for reasons unrelated to law enforcement, in notifying those whose PII had been accessed.

49. As details continue to emerge regarding the November 2014 hack, it has become increasingly apparent that Sony Pictures' culture of complacency with regards to data security, negligence, and willingness to put employees' and customers' PII at risk, resulted in the release of at least 47,000 individuals' personal, sensitive information into the hands of criminals. Plaintiff and class members, including their dependents whose information was also exposed, remain in the dark about the full extent of the breach and their exposure to it.

Sony Pictures Failed to Protect PII Despite Warning Signs

50. As evidenced by Sony's actions prior to the recent data breach, Sony had a pattern and practice of failing to heed warnings to secure its networks, including the failure to implement safeguards sufficient to protect the personal information stored on its servers. For example, over the past 12 years, according to an analysis by security firm Packet Ninjas, more than 900 domains

apparently related to the company have been compromised.[30]

51. In 2007, Jason Spaltro, then-executive director of information security (and now senior vice president of information security) at Sony Pictures Entertainment, gave an interview with CIO Magazine where he was surprisingly flippant about data security at Sony Pictures. He defended that it was a "valid business decision to accept the risk" of a security breach, and contended that he would not invest $10 million to avoid a possible $1 million loss; yet in the same interview, he noted that "Sony is over-compliant in many areas" and that the company takes "the protection of personal information very seriously and invests heavily in controls to protect it."[31]

52. Most famously, in April 2011, Sony's Playstation video game network was massively breached, the first of many recent warning signs. The hack exposed the personal details of 77 million accounts and forced Sony to turn off the network for nearly three weeks. The following month, Sony Corporation's Chief Information Officer, Shinji Hasejima, revealed that the attack had exploited a "known vulnerability,"[32] but assured that it would implement new security measures to prevent against new attacks in the future, including a new data center with "more advanced security," enhanced detection capabilities, automated software monitoring, enhanced data encryption, and additional firewalls. Additionally, Sony would hire a "Chief Information

[30] *See* PacketNinjas, "Sony Pictures Hack Not The Company's First Time With Security Problems," http://logfile.packetninjas.net/sony-pictures-hack-not-the-companys-first-time-with-security-problems/ (last visited Dec. 17, 2014).

[31] http://fusion.net/story/31469/sony-pictures-hack-was-a-long-time-coming-say-former-employees/ http://www.cio.com/article/2439324/risk-management/your-guide-to-good-enough-compliance.html

[32] *See* The Register, "Sony: 'PSN attacker exploited known vulnerability'," http://www.theregister.co.uk/2011/05/01/psn_service_restoration/ (last visited Dec. 17, 2014).

Security Officer" to handle such preparations and to avoid future issues.[33]

53. However, nearly a month after the Playstation attack, an internet security researcher and expert, John Bumgarner, chief technology officer for the U.S. Cyber Consequences Unit (a research group funded by government and private sector grants that monitors Internet threats) still found security flaws in Sony's systems following the April 2011 attack, merely by using a web browser, Google, and a rudimentary understanding of Internet security systems. His research also showed Sony's systems' problems were more widespread than the company has acknowledged; Bumgarner discovered that the flaws were not limited to PlayStation and Sony Online Entertainment systems as Sony had stated,[34] but also found throughout Sony's networks, including Sony Corporation of America and Sony Pictures Entertainment.

54. On June 8, 2011, when asked whether Sony had changed its security systems following the April 2011 breach, Sony's Deputy President Kazuo Hirai stated that Sony has "done everything to bring our practices at least in line with industry standards or better," essentially admitting that when the Playstation breach occurred, its network failed to meet minimum security standards.[35] Just days prior to the admission, hackers breached Sony Pictures Entertainment's websites and allegedly accessed over 1 million people's unencrypted personal information, including customer passwords.[36]

---

[33] *See* Engadget, "Sony's Kaz Hirai addresses PlayStation Network hack, we're liveblogging," http://www.engadget.com/2011/05/01/sonys-kaz-hirai-will-address-playstation-network-hack-at-1am-et/ (last visited Dec. 17, 2014).

[34] http://www.reuters.com/article/2011/05/13/us-sony-idUSTRE74C70420110513

[35] *See* The Guardian, "E3 2011: Sony's Kaz Hirai on the PSN hack," http://www.theguardian.com/technology/2011/jun/08/e3-2011-sony-psn (last visited Dec. 17, 2014).

[36] *See* Mashable, "Sony Pictures Website Hacked, 1 Million Accounts Exposed," http://mashable.com/2011/06/02/sony-pictures-hacked/ (last visited Dec. 17, 2014).

55. Sony characterized the Playstation Network intrusions as highly targeted and sophisticated attacks, but commentators disagreed, starting that the ensuing attacks since the initial April and June 2011 hacks "appear to have been the result of some fundamental security overnights on the part of the company. Several of the attacks have resulted from SQL injection flaws that hackers have claimed were extremely easy to find and to exploit."[37]

56. Numerous class action lawsuits followed the April 2011 Playstation breach, and Sony eventually agreed to a settlement, which has been preliminarily approved, for approximately $15 million in games, online currency, and identity theft reimbursement for affected users.

57. Although Sony Corporation has a history of bringing in top-notch executives in the role of Chief Information Security Officer, these picks did not translate to any enhancement of Sony Pictures' security systems. A number of archaic systems have been in place for ages, making the company's network extremely vulnerable to many angles of attack.[38]

58. Ensuing breaches were kept internal and were not disclosed to the public news media. For example, on or about January 16, 2014, an email from Courtney Schaberg, vice president of legal compliance at Sony Pictures, to general counsel Leah Weil, reported a security compromise of the German Sonypictures.de website. The site was immediately shut down after the company learned that the website had been hacked to distribute malware to visitors. Schaberg expressed concern that email addresses and birthdates for 47,740 individuals who signed up to the site's newsletter had been accessed by the

[37] *Id.*

[38] *See* Ars Technica, "Hackers promise "Christmas present" Sony Pictures won't like," http://arstechnica.com/security/2014/12/hackers-promise-christmas-present-sony-pictures-wont-like/ (last visited Dec. 17, 2014).

attacker.[39] As German law did not require a disclosure to authorities of the breach or the type of information exposed, as this Sonypictures.de website breach did not involve certain kinds of sensitive data such as banking or healthcare information Sony chose to keep this incident secret.

59. One month later, yet another incident was covered up by Sony Pictures executives: a hack in February 2014 affecting the personal data of approximately 760 individuals connected to Sony distributors and theaters in Brazil. A Sony Pictures' server used in connection with SpiritWORLD, the company's international theatrical sales and distribution system, was attacked; yet Sony Pictures only became aware of the breach when a reporter disclosed that thousands of logins were being passed around in online forums. In response, Jason Spaltro, Sony Pictures' executive director of information security, wrote in an email dated February 12, 2014, that while the server itself had not been compromised, a significant amount of payment information for Brazilian film distributors was stolen off the server. Most appallingly, the system, which stored invoice and payment confirmation information as .txt text files, was one which had been in use since 2008.[40]

60. In an email on February 14, 2014, Sony Pictures' vice president of legal compliance, Courtney Schaberg, again minimized the significance of the attack in Brazil: "In terms of a notification obligation, Brazil does not have a breach notification law . . . . [B]ased on the facts known thus far I recommend against providing any notification to individuals given a) the lack of a notification requirement; b) the limited data fields involved [name, address, and

[39] *See* Forbes, "Yet Another Sony Breach Went Unreported In January As 47,740 Individuals' Data Exposed," http://www.forbes.com/sites/thomasbrewster/2014/12/15/sony-pictures-germany-hacked-in-january/

[40] *See* Ars Technica, "Hackers promise "Christmas present" Sony Pictures won't like," http://arstechnica.com/security/2014/12/hackers-promise-christmas-present-sony-pictures-wont-like/ (last visited Dec. 17, 2014).

email address]; and c) the fact that notifying would not likely have much effect in terms of mitigating potential damages."[41]

61. In August of 2014, hackers again took the Sony Playstation Network and Sony Entertainment Network offline with a "distributed denial of service" or "DDoS" attack.[42] A Twitter user "@LizardSquad" claimed credit, saying the attack was intended to motivate Sony to spend more money on upgrading its networks.[43]

62. The dissemination of a scathing internal IT assessment of Sony Pictures' network, dated September 25, 2014, further highlighted Sony Pictures' awareness of its many vulnerabilities and subsequent failure to abide by seemingly basic security procedures and fix its issues. In 2013, in a move indicative of its lax security policies, Sony Corporation's failed to develop proper procedures after oversight responsibilities of the monitoring of Sony subsidiaries were transferred from a third-party security vendor to its Global Security Incident Response Team ("GSIRT") in 2013. In theory, the same third-party vendor was to continue to be responsible for implementing various security measures, such as firewalls and intrusion prevention systems, while GSIRT would take over monitoring security overall. However, a leaked company roster indicates that a mere 11 people were assigned to GSIRT,[44] --woefully inadequate for an international, multi-billion dollar media company with thousands of

[41] *See* Gawker, "Sony Was Hacked in February and Chose to Stay Silent," http://gawker.com/sony-was-hacked-in-february-and-chose-to-stay-silent-1670025366

[42] *See* eSecurity Planet, "Sony Networks Taken Down by DDoS Attack," http://www.esecurityplanet.com/network-security/sony-networks-taken-down-by-ddos-attack.html (last visited Dec. 17, 2014).

[43] *See* Law360, "Sony Exec Faces Bomb Scare Following PlayStation Hack," http://www.law360.com/articles/570772/ (last visited Dec. 17, 2014).

[44] *See* Fusion.net, "Sony Pictures Hack Was a Long Time Coming, Say Former Employees," http://fusion.net/story/31469/sony-pictures-hack-was-a-long-time-coming-say-former-employees/ (last visited Dec. 17, 2014).

employees.

63. Additionally, the September report indicated that, after the transfer occurred, a significant number of critical security devices in the Sony Pictures network were no longer being monitored, rendering them "blind to 17% of their environment" between September 2013 and June 2014. The report also warned that "security incidents impacting these network or infrastructure devices may not be detected" or resolved in a timely manner.[45] Inexplicably, GSIRT also chose to stop sending over monitoring reports that Sony Pictures' IT department had been receiving previously, which would have included "information on security threat trending (e.g., common threats across [Sony Pictures]), log monitoring statistics (e.g., total events for a given month and how they are addressed), . . . and a summary of what [Sony Pictures] could do to reduce specific attacks."[46] Without the reports, the IT department was left without access to data that could be essential to preventing a cyberattack.

64. On information and belief, Sony was alerted *at least a year ago* to the risk that hackers had infiltrated its network and were stealing gigabytes of information. Ars Technica, a technology website, suggests that the attack may have begun much earlier this year, stating, "[i]t's clear that those behind the attack **were deep inside Sony's network for a long time** before they set off the malware that erased Sony hard drives [on November 24, 2014]."[47] The hackers were then able to collect significant intelligence on the network from the IT

[45] *See* Network World, "Sony hacked in February, knew about security flaws before data leak," http://www.networkworld.com/article/2859473/microsoft-subnet/sony-hacked-in-feb-knew-about-huge-security-flaws-before-cybersecurity-train-wreck.html (last visited Dec. 17, 2014).

[46] Id.

[47] *See* Ars Technica, "Hackers promise "Christmas present" Sony Pictures won't like," http://arstechnica.com/security/2014/12/hackers-promise-christmas-present-sony-pictures-wont-like/ (last visited Dec. 17, 2014).

department at Sony Pictures, including lists of computers on Sony Pictures' internal networks, spreadsheets including included the location, IP address, and username for over 10,000 computers worldwide on the network. These details enabled the attackers to easily pick out the most vulnerable servers and infrastructure. Among the leaked data was a digital certificate issued by Sony's corporate certificate authority to Sony Pictures that may have been utilized to create the Sony Pictures certificate that was used to sign a later version of the malware that took the company's computers offline. The #GOP hackers have also hinted that they have had access to and may have been harvesting records from Sony Pictures' network for over a year.[48]

65. Additionally, other cybersecurity firms have focused on the fact that data released by the attackers include a number of Sony's private cryptographic keys. Although the #GOP may not have used these particular keys to gain access to Sony Pictures' network, losing control of these keys effectively opens up the company to attackers who use them to get onto encrypted servers. Using these keys, information can also be moved around in ways that might evade intrusion detection systems.

66. In the 2011 Playstation attack, Sony had also lost control of its cryptographic keys, states Kevin Bocek, vice president at Venafi, a cybersecurity company. This raises a red flag as to why Sony Pictures did not protect its cryptographic keys more closely three years later.[49] Changing and keeping track of cryptographic keys is crucial to protecting a network. The November 2014

[48] *See* CSO Online, "The breach at Sony Pictures is no longer just an IT issue," http://www.csoonline.com/article/2854672/business-continuity/the-breach-at-sony-pictures-is-no-longer-just-an-it-issue.html (last visited Dec. 17, 2014).

[49] *See* Bloomberg BusinessWeek, "Experts: Sony Hackers Were Inside the Company Network for a Long Time," http://www.businessweek.com/articles/2014-12-03/sony-hackers-were-inside-the-company-network-for-a-long-time (last visited Dec. 18, 2014).

breach also suggests that Sony has not changed its ways or learned much since 2011, as one "key weakness" was a lack of established security measures between the computers of the various global Sony divisions, which allowed hackers to move with relative ease throughout the corporation.[50]

67. Despite the numerous warning signs to Sony Pictures' network as well as other Sony subsidiaries' networks, Sony Pictures failed to exercise reasonable practices in protecting its employees and contractors' PII, culminating in the November 2014 breach which exposed tens of thousands of victims' sensitive, personal information.

Delayed, Insufficient Notification and Remedy to Victims

68. Sony Pictures' draft breach notification letter dated December 8, 2014, which was filed with the California State Attorney General's office, states that it learned on December 1 that the security of employees' PII was breached and compromised. In the letter, Sony Pictures offered employees and their dependents a meager twelve months of professional identity theft protection via a third-party service provider, AllClear ID. The notification letter referenced an email sent to employees on Wednesday, December 3, 2014, which contained an activation code for enrolling in AllClear ID's identity theft protection services and contact information for identity repair assistance, and offered the identity protection services at no charge.

69. A purported current employee reported to Gizmodo, a technology blog, that "[i]nitially it was just employees, then a few days later they offered to cover dependents, then early this week they sent an email stating that 'alumni' were being offered the coverage."[51]

---

[50] *See* Bloomberg, "Why Sony's Plan to Foil PlayStation-Type Attacks Faltered," http://www.bloomberg.com/news/2014-12-05/why-sony-s-plan-to-foil-playstation-type-attacks-faltered.html (last visited Dec. 18, 2014).

[51] *See* Gizmodo, "I'm a Sony Pictures Employee," http://gizmodo.com/im-a-sony-pictures-employee-1669809607 (last visited: December 17, 2014).

70. The twelve months of identity monitoring, credit monitoring, fraud assistance, and an identity theft insurance policy offered by Sony Pictures is woefully inadequate to protect Plaintiff and the putative class, and their dependents, from identity theft. The damaging effects of the recent data breach on Plaintiff and class members are likely to extend well past one year and may last individuals' entire lifetimes. In particular, because individual SSNs—which are difficult to change, unlike credit card numbers—were compromised, identity thieves may hold onto PII for years to come, which means that the damages may go beyond any immediate financial loss. According to a 2007 GAO Report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once 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.** (emphasis added).

71. Characterizing the cyber-attack on Sony Pictures as "unprecedented . . . not only in the apparent motivation, but the amount and type of information the thieves got their hands on," Neal O'Farrell, executive director at the Identity Theft Council, called the offer of free identity protection for one year "[a] hollow and largely valueless gesture in this case." O'Farrell contends that "The thieves have so much information [that] many of these employees could be dealing with the aftermath for years—long after Sony has moved on from it. **A lifetime of free protection and support would be a minimum, and even that might not be enough.**" (emphasis added).[52]

72. Furthermore, to this day, Sony Pictures has not sent to Plaintiff written notice of the theft of her PII. Nor has Plaintiff received the purported

[52] *See* HealthcareInfoSecurity, "Sony's Breach Notification: The Details," http://www.healthcareinfosecurity.com/sonys-breach-notification-details-a-7682/op-1 (last visited: December 17, 2014).

offer Sony Pictures said it would make to "alumni" for professional identity theft protection services from AllClear ID. Similarly, Plaintiff's husband and her three then-dependents have not received notice from Sony Pictures regarding the security breach, have not been extended an offer of identity theft protection services by Sony Pictures and have not been offered any other form of relief.

73. Since the subject data breach, Plaintiff has expended significant time, effort, and incurred expenses in order to protect her and her family's PII from being used or attempted to be used by unknown third parties to access, use, or alter Plaintiff and her family's bank and credit accounts, and other PII. As mentioned, Plaintiff purchased LifeLock identity theft protection for herself, her husband, and her three dependent children, at a cost of $1028.05 annually.

CLASS ACTION ALLEGATIONS

74. Plaintiff brings this action on her own behalf, as well as on behalf of each and all other persons similarly situated, and thus seeks class certification under Federal Rules of Civil Procedure 23(a), (b)(2), and/or (b)(3).

75. The Class and Sub-Class are defined as:

> **Class**: All persons, including, without limitation, Defendant's current and former employees, contractors and freelancers and dependents of current and former employees, contractors and freelancers, in the United States whose personally identifiable information was compromised as a result of the November 2014 security breach ("Class").
>
> **California Sub-Class**: All persons, including, without limitation, Defendant's current and former employees, contractors and freelancers and dependents of current and former employees, contractors and freelancers, in California whose personally identifiable information was compromised as a result of the November 2014 security breach ("California Sub-Class").

76. Excluded from the Class and Sub-Class are: (1) Defendant, any entity or division in which Defendant has a controlling interest, and their legal representatives, officers, directors, assigns, and successors; (2) the Judge to whom this case is assigned and the Judge's staff; and (3) any Judge sitting in the

presiding state and/or federal court system who may hear an appeal of any judgment entered.

77. Members of the Class and Sub-Class will hereinafter be referred to as "class members."

78. Plaintiff reserves the right to redefine the Class and Sub-Class and to add additional subclasses as appropriate based on discovery and further investigation.

79. There is a well-defined community of interest in the litigation and each sub-class is readily ascertainable.

80. Numerosity: Although the exact number of prospective class members is uncertain and can only be ascertained through appropriate discovery, the number is great enough such that joinder is impracticable. Upon information and belief, Plaintiff estimates there are at least 47,000 members of the Class, an estimate which does not include dependents and other family members of the individual members of the Class. The disposition of prospective class members' claims in a single action will provide substantial benefits to all parties and to the Court. The prospective class members are readily identifiable from information and records in Defendant's possession, custody, or control. Given that Plaintiff and prospective class members' information was contained on Sony Pictures' network files and given that they are or were in an employment or other business relationship with Defendant (and thereby provided personal information, including their names, addresses, SSNs, etc.), ascertaining who is in the Class will be easily determinable.

81. Typicality: The claims of the representative Plaintiff are typical of the claims of the prospective class members, as the representative Plaintiff and the prospective class members' personal, confidential information was collected by Defendant and contained within the Sony Pictures' network. The representative Plaintiff, like all prospective class members, has been damaged by

Defendant's misconduct in that she has incurred or will incur the cost of monitoring and correcting her and her then-dependents' credits and identities, thereby expending time, money, and resources in order to mitigate or reverse the damage caused by Defendant's actions and failures. Furthermore, the factual bases of Sony Pictures' misconduct are common to all prospective class members and represent a common thread resulting in injury to all prospective class members.

82. Commonality: There are numerous questions of law and fact common to Plaintiff and the prospective class members that predominate over any question affecting individual prospective class members. These common legal and factual issues include the following:

(a) Whether the following information about Plaintiff and each member of the Class constitutes Personal Identifiable Information: name, address, telephone number, Social Security Number, date of birth, financial information, medical information, or health insurance information, among other information;

(b) Whether Defendant failed to notify Plaintiff and each member of the Class of the security breach in the most expedient time possible and without unreasonable delay;

(c) Whether, at all times relevant herein, Defendant failed to adequately implement any procedures and policies to protect and secure the personal identifiable information of Plaintiff and each member of the Class;

(d) Whether, at all times relevant herein, Defendant failed to adequately maintain any procedures and policies to protect and secure the personal identifiable information of Plaintiff and each member of the Class;

(e) Whether Defendant owed Plaintiff and each member of the Class a duty of care to implement and maintain reasonable procedures and practices to prevent the disclosure of private employee information;

(f) Whether Defendant breached that duty of care;

(g) Whether Defendant's conduct violated California Civil Code section 1798.80, *et seq.*;

(h) Whether Defendant's conduct violated California Civil Code section 56, *et seq.*;

(i) Whether Defendant's conduct violated the Fair Credit Reporting Act or Fair and Accurate Credit Transactions Act, codified in 16 C.F.R. § 682.3(a);

(j) Whether Defendant's conduct as described herein was negligent;

(k) Whether Defendant's conduct as described herein was reckless;

(l) Whether Defendant owed Plaintiff and each member of the Class a duty of care regarding the hiring, supervision, and retention of their information technology employees and agents;

(m) Whether Defendant breached that duty of care regarding the hiring, supervision, and retention of such employees and agents;

(n) Whether Defendant's information technology employees were unfit or incompetent;

(o) Whether Defendant was negligent in supervising its information technology employees;

(p) Whether Defendant's conduct as described herein was

deceptive, unlawful, or unfair, thereby violating California's Unfair Competition Law ("UCL"), California Business & Professions Code section 17200, *et seq*.; and

(q) Whether Defendant's conduct as described herein caused injury to Plaintiff and each member of the Class.

83. Adequate Representation: Plaintiff will fairly and adequately protect prospective class members' interests. Plaintiff has retained attorneys experienced in prosecuting class actions, including data breach class actions, and Plaintiff intends to prosecute this action vigorously.

84. Superiority: Plaintiff and the prospective class members have all suffered and will continue to suffer harm and damages as a result of Defendant's unlawful and wrongful conduct. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Absent a class action, prospective class members would likely find the cost of litigating their claims prohibitively high and would therefore have no effective remedy at law. Because of the relatively small size of the individual prospective class members' claims, it is likely that only a few prospective class members could afford to seek legal redress for Defendant's misconduct. Absent a class action, prospective class members will continue to incur damages, and Defendant's misconduct will continue without remedy. Class treatment of common questions of law and fact would also be a superior method to multiple individual actions or piecemeal litigation in that class treatment will conserve the resources of the courts and the litigants and will promote consistency and efficiency of adjudication.

FIRST CAUSE OF ACTION

Violation of California Civil Code § 1798.80, *et seq*.

(Brought on Behalf of Plaintiff and the California Sub-Class)

85. Plaintiff incorporates by reference and re-alleges as if fully stated herein each and every allegation set forth above.

86. The California Legislature enacted California Civil Code section 1798.80, *et seq.* with the specific purpose of ensuring "that personal information about California residents is protected" and to ensure that businesses take appropriate actions following security data breaches to notify affected California residents and mitigate the harm from security data breaches.

87. Civil Code section 1798.81 provides

> The Legislature declares that the right to privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that all individuals have a right of privacy in information pertaining to them. The Legislature further makes the following findings:
>
> (a) The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies.
>
> (b) The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information.
>
> (c) In order to protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits.

88. Civil Code section 1798.81.5(a) expressly provides that its purpose "is to encourage businesses that own or license personal information about Californians to provide reasonable security for that information."

89. Civil Code section 1798.81.5(b) provides

> A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

90. Civil Code section 1798.81.5(c) further provides

> A business that discloses personal information about a California resident pursuant to a contract with a nonaffiliated third party shall require by contract that

> the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.

91. The statute applies to any business that retains personal information for the purpose of using that information in transactions with the person to whom the information relates. Defendant, as a corporation, is a "business" within the meaning of California Civil Code section 1798.80(a).

92. Plaintiff and class members are "individuals" within the meaning of California Civil Code section 1798.80(c).

93. At all relevant times, Defendant retained Plaintiff's and class members' personal information for the purpose of using that information in transactions with Plaintiff and class members relating to their employment and/or health benefits. As such, Defendant "owns or licenses" personal information about Plaintiff and class members within the meaning of Civil Code section 1798.81.5(a).

94. At all relevant times, Defendant retained Plaintiff's and class members' personal identifying information ("PII"). Section 1798.80(e) states that PII includes, without limitation, an individual's name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.

95. In 2002, in response to the ever-growing threat of identity theft, the California legislature enacted Senate Bill 1386, which imposed new obligations on businesses to promptly notify those affected by security breaches. In passing the law, California lawmakers recognized that early notification to affected individuals was crucial to combat the effects of stolen personal information.

Indeed, "[a]ccording to the Attorney General, victims of identity theft must act quickly to minimize the damage; therefore expeditious notification of possible misuse of a person's personal information is imperative." (Sen. Bill No. 1386 (2002-2003 Reg. Sess.) § 1.)

96. Senate Bill 1386, codified at Civil Code section 1798.82(a), imposes a duty on businesses that maintains computerized data containing personal information to disclose any security breach in an expeditious manner to the persons whose personal information was disclosed, or believed to have been disclosed.

97. Civil Code section 1798.82 states, in relevant part,

> (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most ***expedient time possible and without unreasonable delay***…" (Emphasis added.)
>
> (b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
>
> (d) Any person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:
>
> (1) The security breach notification shall be written in plain language.
>
> (2) The security breach notification shall include, at a minimum, the following information:
>
> (A) The name and contact information of the reporting person or business subject to this section.
>
> (B) A list of the types of personal information that were or are reasonably believed to have been the subject of a

> breach.
>
> (C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.
>
> (D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
>
> (E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.
>
> (F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

98. Defendant failed to implement and maintain reasonable security procedures and practices to protect Plaintiff's and class members' PII from unauthorized access and public disclosure. Further, once Defendant had reason to believe that Plaintiff's and class members' personal information had been accessed by unauthorized persons, Defendant had an obligation to expeditiously notify Plaintiff and class members of the security breach, which it failed to do.

99. Upon information and belief, Defendant was aware of the threat of the November 2014 security breach as early as one year ago. Upon information and belief, Defendant discovered the security breach months before it notified current employees of the breach. Despite this knowledge, which Defendant alone was in a position to know, Defendant unreasonably delayed notifying those members of the class who are current employees of the security breach. Further, Defendant has failed to notify Plaintiff and those class members who are not Defendant's current employees of the security breach altogether.

100. Despite the fact that numerous media outlets and news sources have reported that Plaintiff's and other class members' personal information was accessed and publicly disclosed in the November 2014 security breach,

Defendant still has not provided Plaintiff and other class members with information regarding the security breach. As of the date of this Complaint, Defendant has not notified Plaintiff of the security breach.

SECOND CAUSE OF ACTION

Negligence

(Brought on Behalf of Plaintiff and the Class)

101. Plaintiff incorporates by reference and re-alleges as if fully stated herein each and every allegation set forth above.

102. Defendant owed Plaintiff and the Class a duty to protect their private PII.

103. Defendant was aware of a standard or "best practice" in the industry when it came to protecting the private information of current and former employees, contractors, and freelancers. Sony Pictures was aware of the need to protect the PII of its employees and other individuals with whom they dealt with in a business capacity.

104. Defendant breached this duty by failing to take adequate measures to safeguard this information and failed to maintain reasonable security procedures and practices appropriate to protect the PII of Plaintiff and the Class. Defendant failed to adhere to reasonable and appropriate business practices regarding the PII of Plaintiff and the Class, including, but not limited to, storing the PII of Plaintiff and the Class beyond the time necessary and failing to properly ensure that all PII was encrypted or otherwise reasonably safeguarded.

105. Defendant failed to exercise due care. As a direct and proximate result of Defendant's breach of its duties, Plaintiff and the Class have been injured and harmed because Defendant's act and/or omissions resulting in the compromise of their PII has placed them at increased risk of identity theft. Plaintiff and the Class have suffered damages; they have spent and will continue to spend time and/or money in the future to protect themselves as a result of

Defendant's conduct.

THIRD CAUSE OF ACTION

Violations of Cal. Civ. Code § 56, *et seq.* (Confidentiality of Medical Information Act)

(Brought on Behalf of Plaintiff and the California Sub-Class)

106. Plaintiff incorporates by reference and re-alleges as if fully stated herein each and every allegation set forth above.

107. The Confidentiality of Medical Information Act ("CMIA"), codified at California Civil Code section 56, *et seq.* was enacted by California lawmakers.

108. At all relevant times, California Civil Code section 56.20 provides that any employer who receives medical information must establish appropriate procedures to ensure the confidentiality and protection from unauthorized use and disclosure of that information. Section 56.20 further provides that "these procedures may include, but are not limited to, instruction regarding confidentiality of employees and agents handling files containing medical information, and security systems restricting access to files containing medical information.

109. Disclosure of an employee's medical information by an employer is permissible under the CMIA only where the employer has obtained a valid authorization from the employee to disclose the information.

110. At all relevant times, and as stated above, Defendant failed to implement adequate security systems to prevent the disclosure of Plaintiff's and class members' medical information. As a result, Plaintiff's and class members' highly sensitive and private health information was wrongfully accessed and publicly leaked online without their authorization.

111. Pursuant to section 56.35, Plaintiff and Class Members are entitled to compensatory damages, punitive damages not to exceed three thousand dollars ($3,000), attorneys' fees not to exceed one thousand ($1,000), and costs of

litigation arising from Defendant's violation of Civil Code section 56.20.

FOURTH CAUSE OF ACTION

Violations of 15 U.S.C. § 1681w and 16 C.F.R. § 682, *et seq*. (Fair and Accurate Credit Transactions Act)

(Brought on Behalf of Plaintiff and the Class)

112. Plaintiff incorporates by reference and re-alleges as if fully stated herein each and every allegation set forth above.

113. Plaintiff incorporates by reference and re-alleges as if fully stated herein each and every allegation set forth above.

114. The Fair Credit and Reporting Act ("FCRA") requires that any person that maintains or otherwise possesses consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose properly dispose of such information or compilation. 15 U.S.C. § 1681w.

115. Pursuant to the FCRA, the Fair and Accurate Credit Transactions Act of 2003 ("FACTA) was enacted to reduce the risk of consumer fraud and related harms, including identity theft, created by improper disposal of consumer information. FACTA applies to any person over which the Federal Trade Commission has jurisdiction, that, for a business purpose, maintains or otherwise possesses consumer information. 16 C.F.R § 682.2(b).

116. Under FACTA, "any person who maintains or otherwise possesses consumer information for a business purposes must properly dispose of such information ***by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal***." 16 C.F.R § 682.2(b) (Emphasis added).

117. "Consumer Information" is defined under the Act as "any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report. "Consumer report" is

defined by the FCRA as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for … employment purposes." 15 U.S.C. § 1681(d)(1).

118. Consumer information also means a compilation of such records." 16 C.F.R § 682.1(b). "Dispose," "disposing," or "disposal" are defined as "the transfer of any medium, including computer equipment, upon which consumer information is stored." 16 C.F.R § 682.1(c).

119. FACTA further provides a non-exhaustive list of examples of reasonable measures an employer may take to comply with the law's requirement for proper disposal of consumer information. The rule provides, in relevant part:

> (b) Examples. Reasonable measures to protect against unauthorized access to or use of consumer information in connection with its disposal include the following examples. These examples are illustrative only and are not exclusive or exhaustive methods for complying with the rule in this part.
>
> (1) Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing consumer information so that the information cannot practicably be read or reconstructed.
>
> (2) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer information so that the information cannot practicably be read or reconstructed.
>
> (3) After due diligence, entering into and monitoring compliance with a contract with another party engaged in the business of record destruction to dispose of material, specifically identified as consumer information, in a manner consistent with this rule. In this context, due diligence could include reviewing an

> independent audit of the disposal company's operations and/or its compliance with this rule, obtaining information about the disposal company from several references or other reliable sources, requiring that the disposal company be certified by a recognized trade association or similar third party, reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the potential disposal company.
>
> (4) For persons or entities who maintain or otherwise possess consumer information through their provision of services directly to a person subject to this part, implementing and monitoring compliance with policies and procedures that protect against unauthorized or unintentional disposal of consumer information, and disposing of such information in accordance with examples (b)(1) and (2) of this section. 16 C.F.R § 682.3(b).

120. Defendant is subject to jurisdiction of the Federal Trade Commission. Further, Defendant routinely collects and maintains consumer information in the normal course of its business as an employer, including consumer reports, and was therefore required to take reasonable measures to ensure proper disposal of consumer information in its possession regarding Plaintiff and class members.

121. As alleged herein, Defendant did not take reasonable steps to protect and safeguard highly sensitive PII of Plaintiff and class members, including their consumer information. Defendant's failure to protect and safeguard Plaintiff and class members' consumer information, including, but not limited to, background checks obtained in connection with employment applications, violates section 682.2(b).

FIFTH CAUSE OF ACTION

Negligent Hiring, Supervision and/or Retention

(Brought on Behalf of Plaintiff and the Class)

122. Plaintiff incorporates by reference and re-alleges as if fully stated herein each and every allegation set forth above.

123. At all relevant times, Defendant owed Plaintiff and class members a duty of care regarding the hiring, supervision, and retention of their employees and agents.

124. Upon information and belief, Defendant hired, retained and/or supervised various information technology employees charged with the responsibility of securing Defendant's network, including servers and shared drives.

125. Upon information and belief, Defendant's information technology employees were unfit and/or incompetent to perform the work for which they were hired and/or retained, namely, to implement and/or build security infrastructures to protect information maintained on Defendant's network, including servers and shared drives, including Plaintiff and class members' personal identifying information.

126. Alternatively, upon information and belief, Defendant was negligent in supervising their information technology employees hired and/or retained to implement and/or build security infrastructures to protect information maintained on Defendant's network, including servers and shared drives, including Plaintiff and class members' personal identifying information.

127. Defendant knew or should have known that its employees were unfit and/or incompetent and that this unfitness and/or incompetence created a particular risk to Plaintiff and class members who entrusted Defendant to keep their personal identifying information safe and secure.

128. As a result of Defendant's carelessness and recklessness in the retention, hiring and supervision of said employees responsible for implementing safeguards to protect Plaintiff and class members' personal identifying information, Plaintiff and class members have suffered harm or will suffer harm.

129. Defendant's negligence in retaining, hiring and/or supervising said employees was a substantial factor in causing harm to Plaintiff and class

members.

SIXTH CAUSE OF ACTION

(Violation of California Business & Professions Code § 17200, *et seq.*

(Brought on Behalf of Plaintiff and the California Sub-Class)

130. Plaintiff incorporates by reference and re-alleges as if fully stated herein each and every allegation set forth above.

131. Plaintiff brings this cause of action on behalf of herself and on behalf of the California Sub-Class.

132. California Business & Professions Code section 17200 prohibits acts of "unfair competition," including any "unlawful, unfair or fraudulent business act or practice."

133. Defendant's acts, conduct, and practices constitute unlawful and unfair business practices prohibited by Business & Professions Code section 17200.

134. Specifically, Defendant's acts, conduct, and practices were unlawful, in that they constituted violations of the California Security Breach Notification Act; violations of the California Confidentiality of Medical Information Act; and violation of the Fair and Accurate Credit Transactions Act, as described herein.

135. Defendant's acts, conduct, and practices were unlawful and violated California Security Breach Notification Act, Civil Code section 1798.80, *et seq.*, because Sony failed to implement and maintain reasonable security procedures and practices to protect Plaintiff's and class members' personal identifiable information from unauthorized access and public disclosure. Further, once Defendant had reason to believe that Plaintiff's and class members' personal information had been accessed by unauthorized persons, Defendant failed to expeditiously notify Plaintiff and class members of the security breach.

136. Defendant's acts, conduct, and practices were unlawful and violated

the California Confidentiality of Medical Information Act, Civil Code section 56, *et seq.*, because Defendant failed to implement adequate security systems to prevent the disclosure of Plaintiff and class members' medical information, and information was, in fact, released.

137. Defendant's acts, conduct, and practices were unlawful and violated Fair and Accurate Credit Transactions Act, 15 U.S.C. § 1681w and 16 C.F.R. § 682, *et seq.*, because Defendant failed to take reasonable steps to protect and safeguard highly sensitive PII of Plaintiff and class members, including their consumer information.

138. By its conduct, Defendant has engaged in unfair competition and unlawful and unfair business practices.

139. By unnecessarily delaying notification to Plaintiff and class members and/or failing to provide timely notice at all, Defendant engaged in business practices that were unfair and its conduct undermined California public policy.

140. The harmful impact upon the public, the Plaintiff, and the class members resulting from Defendant's conduct as described herein far outweighs any justification by Defendant for such business practices.

141. As a direct and proximate result of Defendant's unfair and unlawful practices, Plaintiff and the Class have suffered and will continue to suffer actual damages.

142. Defendant has been unjustly enriched and should be required to make restitution to Plaintiff and the Class pursuant to §§ 17203 and 17204 of the Business & Professions Code.

PRAYER FOR RELIEF

143. Plaintiff, on behalf of herself, and all others similarly situated, request the Court to enter judgment against Defendant, as follows:

144. Plaintiff, on behalf of herself, and all others similarly situated,

request the Court to enter judgment against Defendant, as follows:

(a) An order certifying the proposed Class, designating Plaintiff as named representative of the Class, and designating the undersigned as Class Counsel;

(b) An award of declaratory and injunctive relief as permitted by law or equity, including: ordering Defendant to take all reasonable measures to protect against any future security breaches of the kind described by this complaint, ordering Defendant to offer extended and/or enhanced credit monitoring protection to Plaintiff and the Class, ordering Defendant to offer extended and/or enhanced identity theft protection to Plaintiff and the Class, ordering Defendant to provide credit restoration services to Plaintiff and the Class, ordering Defendant to provide identity theft insurance to Plaintiff and the Class, ordering Defendant to comply with the notification requirements set forth in California Civil Code section 1798.80 *et seq.*, ordering Defendant to provide prompter notification of security breaches in the future and on a rolling basis as it discovers employees or other persons are affected by a security breach, ordering Defendant to follow industry standards and best practices relating to securing and protecting personal identifiable information; ordering Defendant to take any other actions necessary to safeguard and protect Plaintiff and the Class, and enjoining Defendant from continuing the unlawful practices as set forth herein;

(c) A declaration that Defendant's conduct is a violation of California Civil Code section 1798.80, *et seq.*;

(d) An order enjoining Defendant from further unlawful activities

in violation of California Civil Code section 1798.80, *et seq.*;

(e) An award to Plaintiff and the Class for actual, compensatory, exemplary, and statutory damages, including interest, in an amount to be proven at trial;

(f) An award of reasonable attorneys' fees and litigation costs;

(g) An award of pre-judgment and post-judgment interest, as provided by law;

(h) Leave to amend the Complaint to conform to the evidence produced at trial; and

(i) Such other relief as may be appropriate under the circumstances.

DEMAND FOR JURY TRIAL

145. Plaintiff demands a trial by jury of any and all issues in this action so triable.

Dated: December 19, 2014

Respectfully submitted,

Capstone Law APC

By: s/ Raúl Pérez
Raúl Pérez
Jordan L. Lurie
Robert Friedl
Tarek H. Zohdy
Cody R. Padgett

Attorney for Plaintiff Marcela Bailey