Khesraw Karmand (Cal. Bar No. 280272)
Matthew J. Preusch (Cal. Bar No. 298144)
kkarmand@kellerrohrback.com
mpreusch@kellerrohrback.com
KELLER ROHRBACK L.L.P.
1129 State Street, Suite 8
Santa Barbara, California 93101
Tel.: (805) 456-1496 / Fax (805) 456-1497

Lynn Lincoln Sarko, *pro hac vice forthcoming*
lsarko@kellerrohrback.com
Gretchen Freeman Cappio, *pro hac vice forthcoming*
gcappio@kellerrohrback.com
Cari Campen Laufenberg, *pro hac vice forthcoming*
claufenberg@kellerrohrback.com
Amy N.L. Hanson, *pro hac vice forthcoming*
ahanson@kellerrohrbak.com
KELLER ROHRBACK L.L.P.
1201 Third Ave., Suite 3200
Seattle, Washington 98101
Tel: (206) 623-1900 / Fax: (206) 623-3384

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

Michael Corona and Christina Mathis, individually and on behalf of others similarly situated, Plaintiffs, v. Sony Pictures Entertainment, Inc., Defendant.	CASE NO. CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

I. INTRODUCTION

Plaintiffs Michael Corona and Christina Mathis ("Plaintiffs"), individually and on behalf of all others similarly situated, alleges the following against Sony Pictures Entertainment, Inc. ("Defendant" or "Sony"), based where applicable on personal knowledge, information and belief, and the investigation and research of counsel.

II. NATURE OF THE ACTION

1. An epic nightmare, much better suited to a cinematic thriller than to real life, is unfolding in slow motion for Sony's current and former employees: Their most sensitive data, including over 47,000 Social Security numbers, employment files including salaries, medical information, and anything else that their employer Sony touched, has been leaked to the public, and may even be in the hands of criminals.

2. At its core, the story of "what went wrong" at Sony boils down to two inexcusable problems: (1) Sony failed to secure its computer systems, servers, and databases ("Network"), despite weaknesses that it has known about for years, because Sony made a "business decision to accept the risk" of losses associated with being hacked; and (2) Sony subsequently failed to timely protect confidential information of its current and former employees from law-breaking hackers who (a) found these security weaknesses, (b) obtained confidential information of Sony's current and former employees stored on Sony's Network, (c) warned Sony

that it would publicly disseminate this information, and (d) repeatedly followed through by publicly disseminating portions of the information that they claim to have obtained from Sony's Network through multiple dumps of internal data from Sony's Network.

3. The security weaknesses in Sony's Network exposed sensitive personal identifying information ("PII") to cyber criminals, who obtained that PII (the "Data Breach"). This PII includes, but is not limited to, current and former employee names, home addresses, telephone numbers, birthdates, Social Security numbers, email addresses, salaries and bonus plans, healthcare records, performance evaluations, scans of passports and visas, reasons for termination, details of severance packages and other sensitive employment and personal information.

4. Sony owed a legal duty to Plaintiffs and the other Class members to maintain reasonable and adequate security measures to secure, protect, and safeguard their PII stored on its Network. Sony breached that duty by one or more of the following actions or inactions: failing to design and implement appropriate firewalls and computer systems, failing to properly and adequately encrypt data, losing control of and failing to timely re-gain control over Sony Network's cryptographic keys, and improperly storing and retaining Plaintiffs' and the other Class members' PII on its inadequately protected Network.

5. As the result of Sony's failure to secure its Network, Plaintiffs' and the other Class members' PII was compromised, placing them at an increased risk of fraud and identity theft, and causing direct financial expenses associated with credit monitoring, replacement of compromised credit, debit and bank card numbers, and other measures needed to protect against the misuse of their PII arising from the Data Breach.

6. Sony is no stranger to data breaches, making its vulnerability to this latest attack particularly surprising and egregious. For example, in April 2011, Sony's PlayStation video game network suffered a major breach when hackers stole millions of user accounts from the online gaming service.

7. Given the repeated data breaches suffered by Sony, as well as recent significant data breach events in the retailer context, Sony knew or should have known that such a security breach was likely and taken adequate precautions to protect its current and former employees' PII.

8. In fact, recently leaked emails and internal assessments reveal that Sony's own information technology ("IT") department and, separately, its general counsel believed that its technological security and email retention policies ran the risk of making too much data vulnerable to attack. If only Sony had heeded its own advice in time.

III. JURISDICTION

9. This Court has diversity jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2). Plaintiff Corona and Defendant are citizens of different states. The amount in controversy exceeds $5 million, and there are more than 100 putative class members.

10. This Court has personal jurisdiction over the Defendant because Defendant is licensed to do business in California or otherwise conducts business in California.

11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because unlawful practices are alleged to have been committed in this federal judicial district and Defendant regularly conducts business in this district.

IV. PARTIES

12. Plaintiff Michael Corona is currently a resident of the State of Virginia. Plaintiff Corona is a former employee of Sony Pictures Entertainment. Sony employed Corona from 2004 to 2007 in Culver City, California. Plaintiff Corona's PII was compromised when hackers accessed Sony's Network, including but not limited to his full name, Social Security Number, birthdate, former address, salary history, and reason for resigning. In addition, the PII of Plaintiff Corona's wife and daughter was also compromised in the Data Breach. To date, Plaintiff Corona has incurred costs, including spending over $700 for a year of identity theft protection from LifeLock for him and his family. He has expended 40-50 hours

attempting to safeguard himself and his family members from identity theft or other harms caused by the release of their PII as a result of the Data Breach. Going forward, Plaintiff Corona anticipates spending considerable time each day in an effort to contain the impact of Sony's Data Breach on himself and his family members.

13. Plaintiff Christina Mathis is a resident of the State of California who is temporarily working on an assignment out of state. Plaintiff Mathis is a former employee of Sony Pictures Consumer Products, a subsidiary of Sony. Sony employed Plaintiff Mathis from 2000 to 2002 in Culver City, California. Despite the fact that she has not worked for Sony in 12 years, Plaintiff Mathis's PII was compromised when hackers accessed Sony's Network, including but not limited to her Social Security Number and former address. To date, Plaintiff Mathis has heard nothing from Sony about the breach other than a form letter response to her email inquiry about the Data Breach. Plaintiff Mathis has incurred costs, including spending over $300 for a year of identity theft protection from LifeLock for herself. She has already expended 10 hours attempting to safeguard herself from identity theft and other harms caused by the release of her PII as a result of the Data Breach. Going forward, Plaintiff Mathis anticipates spending considerable time each day in an effort to contain the impact of Sony's Data Breach on herself.

14. Defendant Sony Pictures Entertainment, Inc. is a Corporation organized under the laws of Delaware, with principal offices located in Culver City, County of Los Angeles, California.

V. FACTUAL ALLEGATIONS

A. Sony's Data Breach Exposed the PII of Its Current and Former Employees

15. On information and belief, on November 24, 2014, a hacker group that calls themselves Guardians of Peace ("GOP") took over Sony's Network, displayed their own messages and skeleton image, seized control of promotional Twitter accounts for Sony movies, and warned Sony that it had obtained "secrets" and threatened to leak them to the Web:

16. In the days following the Data Breach, PII of current and former Sony employees, as well as actors and filmmakers were publicly published on the internet.

17. Specifically, on December 2, 2014, data containing the PII of thousands of Sony employees, including, for example, their names, social security

numbers, birthdates, home addresses, job titles, performance evaluations, scans of passports and visas, salaries and bonus plans, reasons for termination and details of severance packages, was posted online.

18. Security researcher Brian Krebs, who was the first to uncover other recent high-profile data breaches at companies such as Target Corporation and Home Depot Inc., reported in a December 2, 2014 blog post that several of his sources had confirmed that the hackers of Sony's Network had stolen more than 25 gigabytes of sensitive data, including Social Security numbers and medical and salary information, on tens of thousands of Sony employees.

19. Krebs reported that he had personally seen several files containing personal information on Sony employees being traded on online torrent networks. The files include a Microsoft Excel document that contains the name, location, employee ID, network username, base salary and date of birth for more than 6,800 people; a status report from April 2014 listing the names, dates of birth, Social Security numbers and health savings account data on more than 700 Sony employees; and a file that appears to be the product of an internal audit from Pricewaterhouse Coopers, made up of screen shots of dozens of employees' federal tax records and other compensation data. Krebs found that a "comprehensive search on LinkedIn for dozens of names in the [Microsoft Excel] list indicate[d] that virtually all correspond[ed] to current or former Sony employees."

20. On the evening of December 2, 2014, sources reported that Sony CEO Michael Lynton and co-chairman Amy Pascal at Sony sent an internal memo to 6,500 current employees that confirmed that a "large amount of confidential Sony Pictures Entertainment data has been stolen by the cyber attackers, including personnel information," stated that "the privacy and security of our employees are of real concern to us," warned that "we are not yet sure of the full scope of information that the attackers have or might release" and "unfortunately have to ask you to assume that information about you in the possession of the company might be in their possession," and promised employees that they would receive an email on December 3, 2014 that outlined steps to sign up for identity protection services.

21. On December 5, 2014, sources reported that Sony's current Data Breach had leaked even more PII than had been reported previously, consisting of 47,426 unique Social Security numbers and names, dates of birth, home addresses, email addresses, salary information, including Social Security numbers of more than 15,200 current or former Sony employees. The Social Security numbers were copied more than 1.1 million times throughout the 601 files stolen by hackers according to Identity Finder LLC, whose company analyzed the breached data. The personal information was found in more than 500 spreadsheets, 75 PDFs and several Word documents, none of which were protected by passwords. Identity Finder LLC CEO Todd Feinman explained that personal information such as

Social Security numbers should be stored in one place with password protection and "[l]eaving these files open is not making the hackers' job difficult." The files have since been publicly posted online on multiple filesharing websites.

22. Also on December 5, 2014, hackers were reported to have sent an email to employees that threatened their families if they did not support Guardians of Peace goals, stating: "Please sign your name to object the false [sic] of the company at the email address below if you don't want to suffer damage. If you don't, not only you but your family will be in danger."

23. As of December 8, 2014, hackers had released around 140 gigabytes of a cache of internal Sony files and films they claim totals at least 100 terabytes—approximately 10 times the amount of information stored in the Library of Congress.

24. Moreover, *Business Insider* reported that Sony CEO Michael Lynton sent a second company-wide memo to current employees on December 8, 2014 assuring them that Sony was doing everything it could to protect employees after a series of cyber-attacks that revealed their personal information, including Social Security numbers and addresses, stating that the Federal Bureau of Investigation has "dedicated their senior staff to this global investigation" and that "recognized experts are working on this matter and looking out for our security."

25. While more than 117,000 cyber-attacks hit businesses each day, the *Los Angeles Times* reported that Phillip Lieberman, the president of security

management program maker Lieberman Software, said few of those attacks are on the scale of the blow dealt to Sony. "It's obvious from the scope of what's been done that the intruders owned the entire environment . . . Sony lost control of their environment," Lieberman said.

26. No definitive evidence about the perpetrators has been disclosed, but several security firms have focused on the fact that data released by the attackers include a number of Sony's private cryptographic keys. Kevin Bocek, vice president at Venafi, explained to *Businessweek* that losing control of these cryptographic "keys to the kingdom" is "a big deal." Once an attacker has access to the cryptographic keys, an attacker can get onto encrypted servers without triggering intrusion detection systems because these systems assume that encrypted data is safe.

27. *Businessweek* reported that an attack using cryptographic keys indicates that the hacker likely spent a significant amount of time within the company's network. This is because companies are often slow to change their cryptographic keys, even when they know they are vulnerable.

28. Some reports have suggested that the attackers of Sony's Network may have initiated their attack as early as a year prior to the public disclosures regarding the Data Breach in November, 2014.

29. Thus, anyone with access to the cryptographic keys would have access to Sony's Network until the company managed to change them—a process

that often becomes difficult when companies lose track of all the ways that cryptographic keys are used. For example, Kaspersky Lab points out that a sample of the malware that hackers installed on the Sony Network during the Data Breach showed traces of being signed by a valid digital certificate from Sony. According to the cybersecurity firm:

> The stolen Sony certificates (which were also leaked by the attackers) can be used to sign other malicious samples. In turn, these can be further used in other attacks. . . . Because the Sony digital certificates are trusted by security solutions, this makes attacks more effective . . . We've seen attackers leverage trusted certificates in the past, as a means of bypassing whitelisting software and default-deny policies.

30. Thus, if Sony's cryptographic keys were among the data released, Sony's ability to prevent further unauthorized access to its Network would be severely compromised and additional, if not ongoing, breaches of its Network would be likely.

31. Information technology online publication ARS Technica notably reported that the hackers were able to collect significant intelligence on the Sony Network from Sony's own information technology department. Amongst the files publicly disclosed the second week of December 2014 was a corporate certificate authority that was intended to be used in creating server certificates for Defendant's Information Systems Service (ISS). This corporate certificate

authority may have been used to create the server certificate that was used to sign a later version of the malware that took Sony's Network offline in November 2014.

B. Despite Sony's Longstanding Knowledge of Its Network's Security Weakness, It Made a Business Decision to Accept This Risk Despite Previous Data Breaches

32. Sony has been a longstanding and frequent target for hackers, but it apparently made a business decision to accept the risk of losses associated with being hacked.

33. Put simply, Sony knew about the risks it took with its past and current employees' data. Sony gambled, and its employees – past and current – lost.

34. For example, as reported on the Gizmodo website, just two months before the Data Breach became public, Sony released a scathing internal IT assessment. In the report Sony's IT personnel found basic security protocol went unheeded and what little IT security it did have was plagued with unmonitored devices, miscommunication, and a lack of accountability.

35. Furthermore, to Sony's chagrin, emails from the Defendant's general counsel, Leah Weil, were reportedly leaked as well. Among other topics, the emails voiced concerns about the volume of data available on emails. For example, one reportedly stated, "While undoubtedly there will be emails that need to be retained or stored electronically in a system other than email, many can be deleted, and I am informed by our IT colleagues that our current use of the email system for virtually everything is not the best way to do this."

36. According to an analysis by security firm Packet Ninjas, more than 900 domains that appear to be related to the company have been compromised over the last twelve years.

37. Sony had the ability and know-how to implement and maintain sufficient online security consistent with industry standards as a leader in the computer technology industry.

38. Nevertheless, as reported by the technology and business website CIO, Sony's executive director of information security, Jason Spaltro, made a business decision in November 2005 not to ensure the security of Sony's Network. At that time, an auditor who had just completed a review of Spaltro's security practices told him that Sony had several security weaknesses, including insufficiently strong access controls, which is a key Sarbanes-Oxley requirement.

39. Spaltro subsequently said in a 2007 interview with CIO that he was not willing to put up a lot of money to defend Sony's sensitive information, stating: "It's a valid business decision to accept the risk."

40. CIO reported on April 6, 2007, that Center for Democracy and Technology privacy expert, Ari Schwartz, believed Spaltro's reasoning to be "shortsighted" because the cost of notification is only a small portion of the potential cost of a data breach.

41. In May 2009, reports surfaced that unauthorized copies of Sony's customers' credit cards were emailed to an outside account.

42. In January 2011, hackers made the PlayStation game Modern Warfare 2 unplayable through the PlayStation Network.

C. Sony's Major Data Breach in April 2011

43. In April 2011, Sony's PlayStation video game network suffered a major breach in April 2011 in which hackers stole millions of user accounts from the online gaming service.

44. Two weeks prior to the April 2011 data breach, Sony was anonymously warned of the impending breach:

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

45. Despite this direct threat to imminently breach the Sony Network, Sony failed to implement adequate safeguards to protect it.

46. As reported by Engadget.com, on May 1, 2011, Sony Corporation Chief Information Officer, Shinji Hasejima, admitted during a press conference that Sony's Network was not secure at the time of the April 2011 data breach and stated that the attack was a "known vulnerability."

47. In addition, on June 8, 2011, Sony's Deputy President, reportedly admitted Sony's Network failed to meet minimum security standards at the time of the April 2011 data breach.

48. As reported by the Guardian, Sony's Kaz Hirai stated that Sony has "done everything to bring our practices at least in line with industry standards or better" when asked whether Sony had revised its security systems following the April 2011 data breach.

49. In response to the April 2011 data breach, Sony represented that it implemented basic measures to defend against new attacks, including the following systems that should have been in place prior to April 2011: automated software monitoring; enhanced data encryption; enhanced ability to detect intrusions to the Network, such as an early-warning system to detect unusual activity patterns; and additional firewalls. Additionally, Sony hired a Chief Information Security Officer.

50. Nevertheless, John Bumgarner, Chief Technology Officer of the independent, non-profit research institute United States Cyber-Consequences Unit, found that as of May 10, 2011, unauthorized users could still access internal Sony resources, including security-management tools. Bumgarner's research also showed that the problems with Sony's systems were more widespread than Sony had acknowledged at that time.

51. After the April 2011 breach, Sony offered free identity theft protection, among other benefits, to PlayStation users.

52. *Businessweek* reported that the cause of the April 2011 breach was that Sony lost control of its cryptographic keys—which is also the focus of several security firms investigating the present Data Breach of Sony's Network—and noted that if Sony has again lost control of its cryptographic keys, it raises the question why it had not protected them more closely three years later.

53. Class action litigation on behalf of gamers followed the April 2011 breach and Sony agreed to settle those claims in June 2014 in exchange for $15 million in games, online currency and identity theft reimbursement.

D. Sony's Failure to Prevent Data Breaches Continued After April 2011

54. Consistent with Mr. Bumgarner's research on the extent of problems with the security of Sony's Network, Sony's bad information technology security habits continued.

55. Sony's Network was again breached in June 2011, compromising over 1 million users' personal information, including names, birthdates, email addresses, passwords, home addresses, and phone numbers.

56. The hackers claimed that it was not difficult to breach Sony's Network in June 2011 and that the stolen data was unencrypted.

57. Numerous experts in the field agree and attribute the June 2011 data breach to an unsophisticated method of hacking that would not have been successful if Sony had even the most basic security measures in place.

58. For example, PCWorld technology journalist Tony Bradly observed that Sony "seems to ignore compliance requirements and basic security best practices, so it is basically begging to be attacked." Bradley further advised that companies should follow security "best practices and data security compliance requirements"—and in short—"[d]on't be a Sony."

59. Likewise, Fred Touchette of AppRiver stated: "[t]here is no doubt that Sony needs to spend some major effort in tightening up its network security. This latest hack against them was a series of simple SQL Injection attacks against its web servers. This simply should not have happened."

60. In February 2014, Sony's executive director of information security Jason Spaltro notified Sony Chief Financial Officer David Hendler that a significant amount of payment information had been stolen off of Sony's Network relating to 759 individuals associated with theaters in Brazil. The stolen payment information had been stored as .txt text files and Sony had been storing this type of information this way since 2008.

61. Spalto brushed off the significance of the February 2014 attack from the standpoint of legal exposure and recommended against providing any notification of this breach to individuals.

62. In contrast, Sony took very seriously the threat of denial of service attacks on its business, particularly after what had happened to the Sony

Playstation Network and issued warnings of likely future attacks in March 2014 and April 2014.

63. In August 2014, a month after Sony settled the class action litigation brought by PlayStation gamers as a result of the April 2011 breach—and just months before the GOP hackers took responsibility for the current Data Breach—hackers again took down the PlayStation Network and also took down Sony's Entertainment Network by overwhelming Sony's Network with "denial of service" attacks.

64. Also in August 2014, information technology online publication ARS Technica reported Sony's Chief Information Security Officer Phil Reitinger announced he would be stepping down, noting that there were a number of archaic systems that had been in place at Sony for ages with plenty of potential attack points.

65. Attacks on Sony's Network have continued to be reported as recently as December 7, 2014.

E. The Federal Government is Currently Investigating Sony's Latest Data Breach

66. On December 1, 2014, the Federal Bureau of Investigation ("FBI") launched an investigation into Sony's cyber-intrusion.

67. The FBI confirmed on December 8, 2014 that it will advise Sony's employees on how to manage the leak of their personal information in the massive Sony Network Data Breach.

68. On December 10, 2014, the Senate Committee on Banking, Housing and Urban Affairs held a cybersecurity hearing in which New York Senator Charles Schumer raised concerns over the origin of Sony's current Data Breach.

F. The Hacked PII of Sony's Current and Former Employees was Valuable

69. As a result of the Data Breach, cyber-criminals now possess the PII of Sony's current and former employees.

70. As the Federal Trade Commission has stated, PII such as Social Security numbers, financial information, and other sensitive information are "what thieves use most often to commit fraud or identity theft." In addition, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."

71. Legitimate organizations and the criminal underground alike recognize the value of such data. Otherwise, they would not pay for or maintain it, or aggressively seek it. Criminals seek personal and financial information of consumers because they can use biographical data to perpetuate more and larger thefts.

G. Sony Failed to Timely and Adequately Protect Current and Former Employees' PII

72. Sony has already acted to protect itself by using hacking methods of its own to combat illegal downloads of its movies that hackers publicly released after the Data Breach, according to Recode. Specifically, it is harnessing Amazon Web Services (the backend that hosts Netflix, Instagram and many others) to launch a distributed denial of service (DDoS) attack on websites hosting the stolen assets.

73. Sony has not, however, similarly acted to protect its current and former employees.

74. This is important because, according to experts, one out of four data breach notification recipients became a victim of identity fraud, in which an identity thief uses another's personal and financial information such as that person's name, address, and other information, without permission, to commit fraud or other crimes.

75. For instance, identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

76. In addition, identity thieves may get medical services using consumers' lost information or commit any number of other frauds, such as obtaining a job, procuring housing or even giving false information to police during an arrest.

77. Furthermore, the PII that Sony failed to adequately protect and that was stolen in the Data Breach is "as good as gold" to identity thieves because identity thieves can use victims' personal data to open new financial accounts and incur charges in another person's name, take out loans in another person's name, and incur charges on existing accounts.

78. Finally, the GOP hackers have already used this PII to harass Sony's employees by threatening harm to their families if they did not cooperate by signing a document evidencing support for the GOP mission and substantially impairing their ability to work while malware was installed on the Sony Network.

79. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

80. Accordingly, as Identity Finder LLC CEO Todd Feinman told Law360, the real victims are Sony's employees and ex-employees: "They're now at risk for identity theft for the rest of their lives."

81. On information and belief, the PII posted to the Internet pertaining to Sony employees was not limited to current employees and dates back to employees

that left Sony as long ago as 2000, and to actors and filmmakers who worked for Sony as far back as 1984.

82. Notably, while several former Sony employees reported seeing their personal data in leaked documents by December 8, 2014, one former high-ranking Sony employee who left the company earlier this year told CNET that: "The studio's done absolutely nothing to reach out to us."

83. On December 9, 2014, on information and belief, Sony began generally responding to inquiries by former Sony employees concerned about the Sony Network Data Breach and public dissemination of former Sony employee PII stolen by the hackers.

84. Sony's belated response did not confirm whether specific current or former employees' PII had been compromised, and instead put the burden on the inquiring current or former employees to act to "minimize your risk of identity theft." Sony's response noted that former Sony employees could expect to receive an email within the next several days that would include instructions on how they could sign up for 12 months of identity protection services at no charge with a third party provider of Sony's choosing.

85. In conjunction with its belated disclosure, Sony put the burden on Plaintiffs and the other Class members to monitor for damages caused by the Data Breach, cautioning them to watch out for unauthorized use of their credit card data and identity-theft scams. Implicitly recognizing the damage caused by the Data

Breach, Sony encouraged Plaintiffs and the other Class members to "remain vigilant, to review your account statements and to monitor your credit reports."

86. On December 10, 2014, Twin Cities.com echoed the concern of former Sony employees, reporting that nearly 4,000 people had joined a recently formed Facebook group called "Sony Ex-Employees Worried about the Info Breach," and that many of those former employees were concerned that they are unable to get information from the studio about how to register for credit monitoring and the identity protection that the studio has now arranged to offer "to all current and potentially affected former employees and their dependents."

87. On information and belief, on or about December 12, 2014, Sony's third party identity protection provider AllClear ID began providing former employees with activation codes that they could use to sign up for credit monitoring and an identity theft insurance policy.

88. Sony's limited offer of 12 months of credit monitoring and insurance is inadequate. Neither does anything to prevent identity fraud. Credit monitoring only informs a consumer of instances of fraudulent opening of new accounts, not fraudulent use of existing credit cards. Agencies of the federal government and privacy experts acknowledge that stolen data may be held for more than a year before being used to commit identity theft and once stolen data has been sold or posted on the Internet, fraudulent use of stolen data may continue for years.

89. On information and belief, the Data Breach to the Sony Network and/or accepting credit monitoring and identity protection may result in credit report agencies placing red flags on current and former Sony employee credit reports, which substantially impairs victims' ability to obtain additional credit.

VI. CLASS ACTION ALLEGATIONS

90. Plaintiffs bring this suit as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of himself and all others similarly situated, as members of a Class initially defined as follows:

> All former and current employees in the United States of Sony whose Personally Identifiable Information was compromised by Sony's security breaches that became public starting in November 2014, and any related security breaches.

91. Plaintiffs also seek to certify a California Subclass consisting of all members of the Class who are residents of California under the respective data breach statute of California set forth in Count III. This class is defined as follows:

> All former and current employees of Sony who are residents of California whose Personally Identifiable Information was compromised by Sony's security breaches that became public starting in November 2014, and any related security breaches.

92. Plaintiffs also seek to certify a Virginia Subclass consisting of all members of the Class who are residents of Virginia under the respective data breach statute of Virginia set forth in Count IV. This class is defined as follows:

> All former and current employees of Sony who are residents of Virginia whose Personally Identifiable Information was compromised by Sony's security breaches that became public starting in November 2014, and any related security breaches.

93. **Numerosity.** The Class is sufficiently numerous, as approximately 15,000 Sony employees and former employees have had their PII compromised. The Putative Class members are so numerous and dispersed throughout the United States that joinder of all members is impracticable. Putative Class members can be identified by records maintained by Defendant.

94. **Common Questions of Fact and Law.** Common questions of fact and law exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class, pursuant to Rule 23(b)(3). Among the questions of fact and law that predominate over any individual issues are:

> (1) Whether Sony failed to exercise reasonable care to protect Plaintiffs' and the Class' PII;
>
> (2) Whether Sony timely, accurately, and adequately informed Plaintiffs and the Class that their PII had been compromised;

(3) Whether Sony's conduct with respect to the data breach was unfair and deceptive;

(4) Whether Sony owed a legal duty to Plaintiffs and the Class to protect their PII and whether Defendant breached this duty;

(5) Whether Sony was negligent;

(6) Whether Sony retains employees' data for a reasonable time;

(7) Whether Plaintiffs and the Class are at an increased risk of identity theft as a result of Sony's breaches and failure to protect Plaintiffs' and the Class' PII; and

(8) Whether Plaintiffs and members of the Class are entitled to the relief sought, including injunctive relief.

95. **Typicality.** Plaintiffs' claims are typical of the claims of members of the Class because Plaintiffs and the Class sustained damages arising out of Defendant's wrongful conduct as detailed herein. Specifically, Plaintiffs' and the Class' claims arise from Sony's failure to install and maintain reasonable security measures to protect Plaintiffs' and the Class's PII, and to timely notify them when the security breach occurred.

96. **Adequacy.** Plaintiffs will fairly and adequately protect the interests of the Class and has retained counsel competent and experienced in class action lawsuits. Plaintiffs have no interests antagonistic to or in conflict with those of the Class and therefore is an adequate representative for Class.

97. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy because the joinder of all members of the putative Class is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of an inconsistent and potentially conflicting adjudication of the claims asserted herein. There will be no difficulty in the management of this action as a class action.

VII. CAUSES OF ACTION

COUNT I: Negligence

98. Plaintiffs and the Class reallege and incorporate by reference the allegations contained in each of the preceding paragraphs of this Complaint as if fully set forth herein.

99. Defendant owed a duty to the Class to exercise reasonable care in obtaining, securing, safeguarding, deleting and protecting Plaintiffs' and the Class' PII within its possession or control from being compromised, lost, stolen, accessed and misused by unauthorized persons. This duty included, among other things, designing, maintaining and testing Sony's security systems to ensure that Plaintiffs' and Class members' PII in Sony's possession was adequately secured and protected. Sony further owed a duty to Plaintiffs and the Class to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warning and alerts including those generated by its own security systems.

100. Sony owed a duty to Plaintiffs and the members of the Class to provide security, including consistent with of industry standards and requirements, to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII of its current and former employees.

101. Sony owed a duty of care to Plaintiffs and the members of the Class because they were foreseeable and probable victims of any inadequate security practices. Sony knew or should have known it had inadequately safeguarded its Network, particularly in light of its multiple prior breaches, as noted above, and yet Sony failed to take reasonable precautions to safeguard current and former employees' PII.

102. Sony owed a duty to timely and accurately disclose to Plaintiffs and members of the Class that their PII had been or was reasonably believed to have been compromised. Timely disclosure was required, appropriate and necessary so that, among other things, Plaintiffs and the members of the Class could take appropriate measures to avoid identify theft or fraudulent charges, including, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions, obtain credit monitoring services, file reports with law enforcement and other governmental agencies and take other steps to mitigate or ameliorate the damages caused by Sony's misconduct.

103. Plaintiffs and members of the Class entrusted Sony with their PII on the premise and with the understanding that Sony would safeguard their

information, and Sony was in a position to protect against the harm suffered by Plaintiffs and members of the Class as a result of the Data Breach.

104. Sony knew, or should have known, of the inherent risks in collecting and storing the PII of Plaintiffs and members of the Class and of the critical importance of providing adequate security of that information.

105. Sony's own conduct also created a foreseeable risk of harm to Plaintiffs and members of the Class. Sony's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent and stop the Data Breach as set forth herein. Sony's misconduct also included its decision not to comply with industry standards for the safekeeping and maintenance of the PII of Plaintiffs and members of the Class.

106. Through its acts and omissions described herein, Sony unlawfully breached its duty to use reasonable care to protect and secure Plaintiffs' and the Class' PII within its possession or control. More specifically, Defendant failed to maintain a number of reasonable security procedures and practices designed to protect the PII of Plaintiffs and the Class, including, but not limited to, establishing and maintaining industry-standard systems to safeguard its current and former employees' PII. Given the risk involved and the amount of data at issue, Sony's breach of its duties was entirely unreasonable.

107. Sony breached its duties to timely and accurately disclose that Plaintiffs' and Class members' PII in Sony's possession had been or was reasonably believed to have been, stolen or compromised.

108. As a direct and proximate result of Defendant's breach of its duties, Plaintiffs and members of the Class have been harmed by the release of their PII, causing them to expend personal income on credit monitoring services and putting them at an increased risk of identity theft. Plaintiffs and members of the Class have spent time and money to protect themselves as a result of Defendant's conduct, and will continue to be required to spend time and money protecting themselves, their identities, their credit, and their reputations.

COUNT II: Violation of California Confidentiality of Medical Information Act, Cal. Civ. Code § 56, *et seq.*

109. Plaintiffs and the Class reallege and incorporate by reference the allegations contained in each of the preceding paragraphs of this Complaint as if fully set forth herein.

110. California Civil Code § 56, *et seq*., known as the Confidentiality of Medical Information Act ("Medical Information Act"), requires employers who receive medical information to establish appropriate procedures to ensure the confidentiality and protection from unauthorized use and disclosure of that information. These procedures may include, but are not limited to, instruction regarding confidentiality of employees and agents handling files containing

medical information, and security systems restricting access to files containing medical information.

111. Furthermore, the Medical Information Act prohibits employers from disclosing medical information regarding a patient without first obtaining written authorization from the patient.

112. In the usual course of business, employers, including Sony, possess and retain certain mediation records and information belonging to its current and former employees, including certain of Plaintiffs' medical information. During their employment with Sony, Plaintiffs lived in California.

113. At all relevant times, Defendant had a legal duty to protect the confidentiality of Plaintiffs' and Class members' medical information.

114. By failing to ensure adequate security systems were in place to prevent access and disclosure of Plaintiffs' and Class members' private medical information without written authorization, Defendant violated the Medical Information Act and their legal duty to protect the confidentiality of such information.

115. Pursuant to Cal. Civ. Code § 56.36, those Plaintiffs and members of the Class whose medical information was compromised are entitled to nominal statutory damages of $1,000 per class member as well as any actual damages sustained by those Plaintiffs and members of the Class.

COUNT III: Violation of Cal. Civ. Code § 1798.80 et seq.
(On Behalf Of Plaintiff Mathis and the California Subclass)

116. Plaintiffs and the Class reallege and incorporate by reference the allegations contained in each of the preceding paragraphs of this Complaint as if fully set forth herein.

117. Section 1798.82 of the California Civil Code provides, in pertinent part, as follows:

> (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.

* * *

(f) Any person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(g) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

118. The unauthorized acquisition of Plaintiffs' and Class members' PII constituted a "breach of the security system" of Sony.

119. Sony unreasonably delayed informing anyone about the breach of security of California Subclass members' confidential and non-public information after Sony knew the Data Breach had occurred.

120. Defendant failed to disclose to California Subclass members, without unreasonable delay, and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, PII when they knew or reasonably believed such information had been compromised.

121. Upon information and belief, no law enforcement agency instructed Sony that notification to California Subclass members would impede investigation.

122. Pursuant to Section 1798.84 of the California Civil Code:

> (a) Any waiver of a provision of this title is contrary to public policy and is void and unenforceable.
>
> * * *
>
> (e) Any business that violates, proposes to violate, or has violated this title may be enjoined.

123. As a result of Sony's violation of Cal. Civ. Code § 1798.82, California Subclass members incurred economic damages relating to expenses for credit monitoring and other identify theft prevention services.

124. Plaintiff Mathis, individually and on behalf of the other California Subclass members, seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to: (a) damages suffered by California Subclass members as alleged above; and (b) equitable relief.

COUNT IV: Violation of § 18.2-186.6., et seq.
(On Behalf Of Plaintiff Corona and the Virginia Subclass)

125. Plaintiffs and the Class reallege and incorporate by reference the allegations contained in each of the preceding paragraphs of this Complaint as if fully set forth herein.

126. Section 18.2-186.6 of the Code of Virginia provides, in pertinent part, as follows:

> (B) If unencrypted or unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person and causes, or the individual or entity reasonably believes has caused or will cause, identity theft or another fraud to any resident of the Commonwealth, an individual or entity 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 of the security of the system to the Office of the Attorney General and any affected resident of the Commonwealth without unreasonable delay. Notice required by this section may be reasonably delayed to allow the individual or entity to determine the scope of the breach of the security of the system and restore the reasonable integrity of the system. Notice required by this section may be delayed if, after the individual or entity notifies a law-enforcement agency, the law-enforcement agency determines and advises the individual or entity that the notice will impede a criminal

or civil investigation, or homeland or national security. Notice shall be made without unreasonable delay after the law-enforcement agency determines that the notification will no longer impede the investigation or jeopardize national or homeland security.

(C) An individual or entity shall disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key and the individual or entity reasonably believes that such a breach has caused or will cause identity theft or other fraud to any resident of the Commonwealth.

(D) An individual or entity that maintains computerized data that includes personal information that the individual or entity does not own or license shall notify the owner or licensee of the information of any breach of the security of the system without unreasonable delay following discovery of the breach of the security of the system, if the personal information was accessed and acquired by an unauthorized person or the individual or entity reasonably believes the personal information was accessed and acquired by an unauthorized person.

(E) In the event an individual or entity provides notice to more than 1,000 persons at one time pursuant to this section, the individual or entity shall notify, without unreasonable delay, the Office of the

Attorney General and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice.

127. For purposes of this section, "personal information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:

(a) Social security number;

(b) Driver's license number or state identification card number issued in lieu of a driver's license number; or

(c) Financial account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.

128. For purposes of this section, "notice" means:

(1) Written notice to the last known postal address in the records of the individual or entity;

(2) Telephone notice;

(3) Electronic notice; or

(4) Substitute notice, if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed $50,000, the

affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or consent to provide notice as described in subdivisions 1, 2, or 3 of this definition. Substitute notice consists of all of the following:

(a) E-mail notice if the individual or the entity has e-mail addresses for the members of the affected class of residents;

(b) Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; and

(c) Notice to major statewide media.

129. Further, the "notice" required by this section shall include a description of the following:

(1) The incident in general terms;

(2) The type of personal information that was subject to the unauthorized access and acquisition;

(3) The general acts of the individual or entity to protect the personal information from further unauthorized access;

(4) A telephone number that the person may call for further information and assistance, if one exists; and

(5) Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.

130. "Breach of the security of the system" means the unauthorized access and acquisition of unencrypted and unredacted computerized data that compromises the security or confidentiality of personal information maintained by an individual or entity as part of a database of personal information regarding multiple individuals and that causes, or the individual or entity reasonably believes has caused, or will cause, identity theft or other fraud to any resident of the Commonwealth. Good faith acquisition of personal information by an employee or agent of an individual or entity for the purposes of the individual or entity is not a breach of the security of the system, provided that the personal information is not used for a purpose other than a lawful purpose of the individual or entity or subject to further unauthorized disclosure.

131. The unauthorized acquisition of Plaintiffs' and Class members' PII constituted a "breach of the security of the system" of Sony under Section 18.2-186.6.A. of the Code of Virginia.

132. Sony unreasonably delayed informing anyone about the breach of security of Virginia Subclass members' confidential and non-public information after Sony knew the Data Breach had occurred.

133. Defendant failed to disclose to Virginia Subclass members, without unreasonable delay, and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, personal information when they knew or reasonably believed such information had been compromised.

134. Upon information and belief, no law enforcement agency instructed Sony that notification to Virginia Subclass members would impede investigation.

135. Nothing in Section 18.2-186.6.I. of the Code of Virginia limits an individual from recovering direct economic damages from a violation of this section.

136. As a result of Sony's violation of Section 18.2-186.6. of the Code of Virginia, Virginia Subclass members incurred economic damages relating to expenses for credit monitoring and identity theft protection. In addition, they have expended many hours attempting to safeguard themselves from identity theft or other harms caused by the release of their PII as a result of the Data Breach, including freezing their credit records and other identify theft prevention services.

137. Plaintiff Corona, individually and on behalf of the other Virginia Subclass members, seek all remedies available under Section 18.2-186.6.I. of the Code of Virginia, including, but not limited to: (a) damages suffered by Virginia Subclass members as alleged above; and (b) equitable relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class set forth herein, respectfully requests the following relief:

A. That the Court certify this case as a class action pursuant to Federal Rule of Civil Procedure 23(a), (b)(2) and (b)(3), and, pursuant to Federal Rule of

Civil Procedure 23(g), appoint Plaintiffs and Plaintiffs' counsel of record to represent said Class;

B. Finding that Sony breached its duty to safeguard and protect Plaintiffs' and the Class' PII that was compromised in the security breach that became public knowledge starting in November 2014;

C. That the Court award Plaintiffs and the Class appropriate relief, including any actual and statutory damages, restitution and disgorgement.

D. That the Court award equitable, injunctive and declaratory relief as may be appropriate under applicable state laws. Plaintiffs, on behalf of the Class seeks appropriate injunctive relief, including but not limited to: (i) the provision of credit monitoring and/or credit card monitoring services for the Class for at least five years; (ii) the provision of bank monitoring and/or bank monitoring services for the Class for at least five years; (iii) the provision of identity theft insurance for the Class for at least five years; (iv) the provision of credit restoration services for the Class for at least five years; (v) awarding Plaintiffs and the Class the reasonable costs and expenses of suit, including attorneys' fees, filing fees, and insurance for the Class; and (vi) requiring that Sony receive periodic compliance audits by a third party regarding the security of its computer systems used for storing current and former employee data, to ensure against the recurrence of a data breach by adopting and implementing best security data practices;

E. Awarding the damages requested herein to Plaintiffs and the Class;

F. Awarding all costs, including experts' fees and attorneys' fees, and the costs of prosecuting this action;

G. Awarding pre-judgment and post-judgment interest as prescribed by law; and

H. Granting additional legal or equitable relief as this Court may find just and proper.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

DATED this 15th day of December, 2014.

KELLER ROHRBACK L.L.P.

By s/ *Khesraw Karmand*

Khesraw Karmand (SBN 280272)
Matthew J. Preusch (SBN 298144)
kkarmand@kellerrohrback.com
mpreusch@kellerrohrback.com
1129 State Street, Suite 8
Santa Barbara, California 93101
Tel.: (805) 456-1496, Fax (805) 456-1497

Lynn Lincoln Sarko, *pro hac vice forthcoming*
lsarko@kellerrohrback.com
Gretchen Freeman Cappio, *pro hac vice forthcoming*
gcappio@kellerrohrback.com
Cari Campen Laufenberg, *pro hac vice forthcoming*
claufenberg@kellerrohrback.com
Amy N.L. Hanson, *pro hac vice forthcoming*
ahanson@kellerrohrbak.com
1201 Third Ave., Suite 3200
Seattle, Washington 98101
Tel: (206) 623-1900 / Fax: (206) 623-3384

Attorneys for Plaintiffs Michael Corona and Christina Mathis