

1 Khesraw Karmand (Cal. Bar No. 280272)
2 Matthew J. Preusch (Cal. Bar No. 298144)
3 kkarmand@kellerrohrback.com
4 mpreusch@kellerrohrback.com
5 **KELLER ROHRBACK L.L.P.**
6 1129 State Street, Suite 8
7 Santa Barbara, California 93101
8 Tel.: (805) 456-1496 / Fax (805) 456-1497

9 Lynn Lincoln Sarko, *pro hac vice forthcoming*
10 lsarko@kellerrohrback.com
11 Gretchen Freeman Cappio, *pro hac vice forthcoming*
12 gcappio@kellerrohrback.com
13 Cari Campen Laufenberg, *pro hac vice forthcoming*
14 claufenberg@kellerrohrback.com
15 Amy N.L. Hanson, *pro hac vice forthcoming*
16 ahanson@kellerrohrbak.com
17 **KELLER ROHRBACK L.L.P.**
18 1201 Third Ave., Suite 3200
19 Seattle, Washington 98101
20 Tel: (206) 623-1900 / Fax: (206) 623-3384

21 **Attorneys for Plaintiffs**

22 **UNITED STATES DISTRICT COURT**

23 **CENTRAL DISTRICT OF CALIFORNIA**

24 Michael Corona and Christina Mathis,) CASE NO.
25 individually and on behalf of others)
26 similarly situated,) CLASS ACTION COMPLAINT
27)
28 Plaintiffs,)
29) JURY TRIAL DEMANDED
30 v.)
31)
32 Sony Pictures Entertainment, Inc.,)
33)
34 Defendant.)

1
2
3
4
5
6
7
8
9
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.

10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
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

1 that it would publicly disseminate this information, and (d) repeatedly followed
2 through by publicly disseminating portions of the information that they claim to
3 have obtained from Sony's Network through multiple dumps of internal data from
4 Sony's Network.
5

6 3. The security weaknesses in Sony's Network exposed sensitive
7 personal identifying information ("PII") to cyber criminals, who obtained that PII
8 (the "Data Breach"). This PII includes, but is not limited to, current and former
9 employee names, home addresses, telephone numbers, birthdates, Social Security
10 numbers, email addresses, salaries and bonus plans, healthcare records,
11 performance evaluations, scans of passports and visas, reasons for termination,
12 details of severance packages and other sensitive employment and personal
13 information.
14
15
16

17 4. Sony owed a legal duty to Plaintiffs and the other Class members to
18 maintain reasonable and adequate security measures to secure, protect, and
19 safeguard their PII stored on its Network. Sony breached that duty by one or more
20 of the following actions or inactions: failing to design and implement appropriate
21 firewalls and computer systems, failing to properly and adequately encrypt data,
22 losing control of and failing to timely re-gain control over Sony Network's
23 cryptographic keys, and improperly storing and retaining Plaintiffs' and the other
24 Class members' PII on its inadequately protected Network.
25
26
27
28

1 5. As the result of Sony’s failure to secure its Network, Plaintiffs’ and
2 the other Class members’ PII was compromised, placing them at an increased risk
3 of fraud and identity theft, and causing direct financial expenses associated with
4 credit monitoring, replacement of compromised credit, debit and bank card
5 numbers, and other measures needed to protect against the misuse of their PII
6 arising from the Data Breach.
7
8

9 6. Sony is no stranger to data breaches, making its vulnerability to this
10 latest attack particularly surprising and egregious. For example, in April 2011,
11 Sony’s PlayStation video game network suffered a major breach when hackers
12 stole millions of user accounts from the online gaming service.
13

14 7. Given the repeated data breaches suffered by Sony, as well as recent
15 significant data breach events in the retailer context, Sony knew or should have
16 known that such a security breach was likely and taken adequate precautions to
17 protect its current and former employees’ PII.
18

19 8. In fact, recently leaked emails and internal assessments reveal that
20 Sony’s own information technology (“IT”) department and, separately, its general
21 counsel believed that its technological security and email retention policies ran the
22 risk of making too much data vulnerable to attack. If only Sony had heeded its own
23 advice in time.
24
25
26
27
28

III. JURISDICTION

1
2 9. This Court has diversity jurisdiction over this action pursuant to the
3 Class Action Fairness Act (“CAFA”), 28 U.S.C. § 1332(d)(2). Plaintiff Corona and
4 Defendant are citizens of different states. The amount in controversy exceeds \$5
5 million, and there are more than 100 putative class members.
6

7
8 10. This Court has personal jurisdiction over the Defendant because
9 Defendant is licensed to do business in California or otherwise conducts business
10 in California.
11

12 11. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because
13 unlawful practices are alleged to have been committed in this federal judicial
14 district and Defendant regularly conducts business in this district.
15

IV. PARTIES

16
17 12. Plaintiff Michael Corona is currently a resident of the State of
18 Virginia. Plaintiff Corona is a former employee of Sony Pictures Entertainment.
19 Sony employed Corona from 2004 to 2007 in Culver City, California. Plaintiff
20 Corona’s PII was compromised when hackers accessed Sony’s Network, including
21 but not limited to his full name, Social Security Number, birthdate, former address,
22 salary history, and reason for resigning. In addition, the PII of Plaintiff Corona’s
23 wife and daughter was also compromised in the Data Breach. To date, Plaintiff
24 Corona has incurred costs, including spending over \$700 for a year of identity theft
25 protection from LifeLock for him and his family. He has expended 40-50 hours
26
27
28

1 attempting to safeguard himself and his family members from identity theft or
2 other harms caused by the release of their PII as a result of the Data Breach. Going
3 forward, Plaintiff Corona anticipates spending considerable time each day in an
4 effort to contain the impact of Sony's Data Breach on himself and his family
5 members.
6

7
8 13. Plaintiff Christina Mathis is a resident of the State of California who
9 is temporarily working on an assignment out of state. Plaintiff Mathis is a former
10 employee of Sony Pictures Consumer Products, a subsidiary of Sony. Sony
11 employed Plaintiff Mathis from 2000 to 2002 in Culver City, California. Despite
12 the fact that she has not worked for Sony in 12 years, Plaintiff Mathis's PII was
13 compromised when hackers accessed Sony's Network, including but not limited to
14 her Social Security Number and former address. To date, Plaintiff Mathis has
15 heard nothing from Sony about the breach other than a form letter response to her
16 email inquiry about the Data Breach. Plaintiff Mathis has incurred costs, including
17 spending over \$300 for a year of identity theft protection from LifeLock for
18 herself. She has already expended 10 hours attempting to safeguard herself from
19 identity theft and other harms caused by the release of her PII as a result of the
20 Data Breach. Going forward, Plaintiff Mathis anticipates spending considerable
21 time each day in an effort to contain the impact of Sony's Data Breach on herself.
22
23
24
25
26
27
28

1 14. Defendant Sony Pictures Entertainment, Inc. is a Corporation
2 organized under the laws of Delaware, with principal offices located in Culver
3 City, County of Los Angeles, California.
4

5 **V. FACTUAL ALLEGATIONS**

6 **A. Sony’s Data Breach Exposed the PII of Its Current and Former**
7 **Employees**

8 15. On information and belief, on November 24, 2014, a hacker group
9 that calls themselves Guardians of Peace (“GOP”) took over Sony’s Network,
10 displayed their own messages and skeleton image, seized control of promotional
11 Twitter accounts for Sony movies, and warned Sony that it had obtained “secrets”
12 and threatened to leak them to the Web:
13
14



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

26 17. Specifically, on December 2, 2014, data containing the PII of
27 thousands of Sony employees, including, for example, their names, social security
28

1 numbers, birthdates, home addresses, job titles, performance evaluations, scans of
2 passports and visas, salaries and bonus plans, reasons for termination and details of
3 severance packages, was posted online.
4

5 18. Security researcher Brian Krebs, who was the first to uncover other
6 recent high-profile data breaches at companies such as Target Corporation and
7 Home Depot Inc., reported in a December 2, 2014 blog post that several of his
8 sources had confirmed that the hackers of Sony's Network had stolen more than 25
9 gigabytes of sensitive data, including Social Security numbers and medical and
10 salary information, on tens of thousands of Sony employees.
11
12

13 19. Krebs reported that he had personally seen several files containing
14 personal information on Sony employees being traded on online torrent networks.
15 The files include a Microsoft Excel document that contains the name, location,
16 employee ID, network username, base salary and date of birth for more than 6,800
17 people; a status report from April 2014 listing the names, dates of birth, Social
18 Security numbers and health savings account data on more than 700 Sony
19 employees; and a file that appears to be the product of an internal audit from
20 Pricewaterhouse Coopers, made up of screen shots of dozens of employees' federal
21 tax records and other compensation data. Krebs found that a "comprehensive
22 search on LinkedIn for dozens of names in the [Microsoft Excel] list indicate[d]
23 that virtually all correspond[ed] to current or former Sony employees."
24
25
26
27
28

1 20. On the evening of December 2, 2014, sources reported that Sony CEO
2 Michael Lynton and co-chairman Amy Pascal at Sony sent an internal memo to
3 6,500 current employees that confirmed that a “large amount of confidential Sony
4 Pictures Entertainment data has been stolen by the cyber attackers, including
5 personnel information,” stated that “the privacy and security of our employees are
6 of real concern to us,” warned that “we are not yet sure of the full scope of
7 information that the attackers have or might release” and “unfortunately have to
8 ask you to assume that information about you in the possession of the company
9 might be in their possession,” and promised employees that they would receive an
10 email on December 3, 2014 that outlined steps to sign up for identity protection
11 services.
12

13 21. On December 5, 2014, sources reported that Sony’s current Data
14 Breach had leaked even more PII than had been reported previously, consisting of
15 47,426 unique Social Security numbers and names, dates of birth, home addresses,
16 email addresses, salary information, including Social Security numbers of more
17 than 15,200 current or former Sony employees. The Social Security numbers were
18 copied more than 1.1 million times throughout the 601 files stolen by hackers
19 according to Identity Finder LLC, whose company analyzed the breached data. The
20 personal information was found in more than 500 spreadsheets, 75 PDFs and
21 several Word documents, none of which were protected by passwords. Identity
22 Finder LLC CEO Todd Feinman explained that personal information such as
23
24
25
26
27
28

1 Social Security numbers should be stored in one place with password protection
2 and “[l]eaving these files open is not making the hackers’ job difficult.” The files
3 have since been publicly posted online on multiple filesharing websites.
4

5 22. Also on December 5, 2014, hackers were reported to have sent an
6 email to employees that threatened their families if they did not support Guardians
7 of Peace goals, stating: “Please sign your name to object the false [sic] of the
8 company at the email address below if you don’t want to suffer damage. If you
9 don’t, not only you but your family will be in danger.”
10

11 23. As of December 8, 2014, hackers had released around 140 gigabytes
12 of a cache of internal Sony files and films they claim totals at least 100 terabytes—
13 approximately 10 times the amount of information stored in the Library of
14 Congress.
15

16 24. Moreover, *Business Insider* reported that Sony CEO Michael Lynton
17 sent a second company-wide memo to current employees on December 8, 2014
18 assuring them that Sony was doing everything it could to protect employees after a
19 series of cyber-attacks that revealed their personal information, including Social
20 Security numbers and addresses, stating that the Federal Bureau of Investigation
21 has “dedicated their senior staff to this global investigation” and that “recognized
22 experts are working on this matter and looking out for our security.”
23

24 25. While more than 117,000 cyber-attacks hit businesses each day, the
25 *Los Angeles Times* reported that Phillip Lieberman, the president of security
26
27
28

1 management program maker Lieberman Software, said few of those attacks are on
2 the scale of the blow dealt to Sony. “It’s obvious from the scope of what’s been
3 done that the intruders owned the entire environment . . . Sony lost control of their
4 environment,” Lieberman said.
5

6 26. No definitive evidence about the perpetrators has been disclosed, but
7 several security firms have focused on the fact that data released by the attackers
8 include a number of Sony’s private cryptographic keys. Kevin Bocek, vice
9 president at Venafi, explained to *Businessweek* that losing control of these
10 cryptographic “keys to the kingdom” is “a big deal.” Once an attacker has access to
11 the cryptographic keys, an attacker can get onto encrypted servers without
12 triggering intrusion detection systems because these systems assume that encrypted
13 data is safe.
14
15
16

17 27. *Businessweek* reported that an attack using cryptographic keys
18 indicates that the hacker likely spent a significant amount of time within the
19 company’s network. This is because companies are often slow to change their
20 cryptographic keys, even when they know they are vulnerable.
21

22 28. Some reports have suggested that the attackers of Sony’s Network
23 may have initiated their attack as early as a year prior to the public disclosures
24 regarding the Data Breach in November, 2014.
25

26 29. Thus, anyone with access to the cryptographic keys would have
27 access to Sony’s Network until the company managed to change them—a process
28

1 that often becomes difficult when companies lose track of all the ways that
2 cryptographic keys are used. For example, Kaspersky Lab points out that a sample
3 of the malware that hackers installed on the Sony Network during the Data Breach
4 showed traces of being signed by a valid digital certificate from Sony. According
5 to the cybersecurity firm:
6

7 The stolen Sony certificates (which were also leaked by the attackers)
8 can be used to sign other malicious samples. In turn, these can be
9 further used in other attacks. . . . Because the Sony digital certificates
10 are trusted by security solutions, this makes attacks more effective . . .
11

12 We've seen attackers leverage trusted certificates in the past, as a
13 means of bypassing whitelisting software and default-deny policies.
14

15 30. Thus, if Sony's cryptographic keys were among the data released,
16 Sony's ability to prevent further unauthorized access to its Network would be
17 severely compromised and additional, if not ongoing, breaches of its Network
18 would be likely.
19

20 31. Information technology online publication ARS Technica notably
21 reported that the hackers were able to collect significant intelligence on the Sony
22 Network from Sony's own information technology department. Amongst the files
23 publicly disclosed the second week of December 2014 was a corporate certificate
24 authority that was intended to be used in creating server certificates for
25 Defendant's Information Systems Service (ISS). This corporate certificate
26
27
28

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

3
4 **B. Despite Sony's Longstanding Knowledge of Its Network's Security**
5 **Weakness, It Made a Business Decision to Accept This Risk Despite**
6 **Previous Data Breaches**

7
8 32. Sony has been a longstanding and frequent target for hackers, but it
9 apparently made a business decision to accept the risk of losses associated with
10 being hacked.

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

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

18
19 35. Furthermore, to Sony's chagrin, emails from the Defendant's general
20 counsel, Leah Weil, were reportedly leaked as well. Among other topics, the
21 emails voiced concerns about the volume of data available on emails. For example,
22 one reportedly stated, "While undoubtedly there will be emails that need to be
23 retained or stored electronically in a system other than email, many can be deleted,
24 and I am informed by our IT colleagues that our current use of the email system for
25 virtually everything is not the best way to do this."
26
27
28

1 36. According to an analysis by security firm Packet Ninjas, more than
2 900 domains that appear to be related to the company have been compromised over
3 the last twelve years.
4

5 37. Sony had the ability and know-how to implement and maintain
6 sufficient online security consistent with industry standards as a leader in the
7 computer technology industry.
8

9 38. Nevertheless, as reported by the technology and business website
10 CIO, Sony's executive director of information security, Jason Spaltro, made a
11 business decision in November 2005 not to ensure the security of Sony's Network.
12 At that time, an auditor who had just completed a review of Spaltro's security
13 practices told him that Sony had several security weaknesses, including
14 insufficiently strong access controls, which is a key Sarbanes-Oxley requirement.
15
16

17 39. Spaltro subsequently said in a 2007 interview with CIO that he was
18 not willing to put up a lot of money to defend Sony's sensitive information, stating:
19 "It's a valid business decision to accept the risk."
20

21 40. CIO reported on April 6, 2007, that Center for Democracy and
22 Technology privacy expert, Ari Schwartz, believed Spaltro's reasoning to be
23 "shortsighted" because the cost of notification is only a small portion of the
24 potential cost of a data breach.
25

26 41. In May 2009, reports surfaced that unauthorized copies of Sony's
27 customers' credit cards were emailed to an outside account.
28

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

3
4 **C. Sony’s Major Data Breach in April 2011**

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

8
9 44. Two weeks prior to the April 2011 data breach, Sony was
10 anonymously warned of the impending breach:

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

16
17
18 45. Despite this direct threat to imminently breach the Sony Network,
19 Sony failed to implement adequate safeguards to protect it.

20
21 46. As reported by Engadget.com, on May 1, 2011, Sony Corporation
22 Chief Information Officer, Shinji Hasejima, admitted during a press conference
23 that Sony’s Network was not secure at the time of the April 2011 data breach and
24 stated that the attack was a “known vulnerability.”
25
26
27
28

1 47. In addition, on June 8, 2011, Sony's Deputy President, reportedly
2 admitted Sony's Network failed to meet minimum security standards at the time of
3 the April 2011 data breach.
4

5 48. As reported by the Guardian, Sony's Kaz Hirai stated that Sony has
6 "done everything to bring our practices at least in line with industry standards or
7 better" when asked whether Sony had revised its security systems following the
8 April 2011 data breach.
9

10 49. In response to the April 2011 data breach, Sony represented that it
11 implemented basic measures to defend against new attacks, including the following
12 systems that should have been in place prior to April 2011: automated software
13 monitoring; enhanced data encryption; enhanced ability to detect intrusions to the
14 Network, such as an early-warning system to detect unusual activity patterns; and
15 additional firewalls. Additionally, Sony hired a Chief Information Security Officer.
16
17

18 50. Nevertheless, John Bumgarner, Chief Technology Officer of the
19 independent, non-profit research institute United States Cyber-Consequences Unit,
20 found that as of May 10, 2011, unauthorized users could still access internal Sony
21 resources, including security-management tools. Bumgarner's research also
22 showed that the problems with Sony's systems were more widespread than Sony
23 had acknowledged at that time.
24
25

26 51. After the April 2011 breach, Sony offered free identity theft
27 protection, among other benefits, to PlayStation users.
28

1 52. *Businessweek* reported that the cause of the April 2011 breach was
2 that Sony lost control of its cryptographic keys—which is also the focus of several
3 security firms investigating the present Data Breach of Sony’s Network—and
4 noted that if Sony has again lost control of its cryptographic keys, it raises the
5 question why it had not protected them more closely three years later.
6

7
8 53. Class action litigation on behalf of gamers followed the April 2011
9 breach and Sony agreed to settle those claims in June 2014 in exchange for \$15
10 million in games, online currency and identity theft reimbursement.
11

12 **D. Sony’s Failure to Prevent Data Breaches Continued After April 2011**

13 54. Consistent with Mr. Bumgarner’s research on the extent of problems
14 with the security of Sony’s Network, Sony’s bad information technology security
15 habits continued.
16

17 55. Sony’s Network was again breached in June 2011, compromising over
18 1 million users’ personal information, including names, birthdates, email
19 addresses, passwords, home addresses, and phone numbers.
20

21 56. The hackers claimed that it was not difficult to breach Sony’s
22 Network in June 2011 and that the stolen data was unencrypted.
23

24 57. Numerous experts in the field agree and attribute the June 2011 data
25 breach to an unsophisticated method of hacking that would not have been
26 successful if Sony had even the most basic security measures in place.
27
28

1 58. For example, PCWorld technology journalist Tony Bradly observed
2 that Sony “seems to ignore compliance requirements and basic security best
3 practices, so it is basically begging to be attacked.” Bradley further advised that
4 companies should follow security “best practices and data security compliance
5 requirements”—and in short—“[d]on’t be a Sony.”
6

7
8 59. Likewise, Fred Touchette of AppRiver stated: “[t]here is no doubt that
9 Sony needs to spend some major effort in tightening up its network security. This
10 latest hack against them was a series of simple SQL Injection attacks against its
11 web servers. This simply should not have happened.”
12

13 60. In February 2014, Sony’s executive director of information security
14 Jason Spaltro notified Sony Chief Financial Officer David Hendler that a
15 significant amount of payment information had been stolen off of Sony’s Network
16 relating to 759 individuals associated with theaters in Brazil. The stolen payment
17 information had been stored as .txt text files and Sony had been storing this type of
18 information this way since 2008.
19

20
21 61. Spalto brushed off the significance of the February 2014 attack from
22 the standpoint of legal exposure and recommended against providing any
23 notification of this breach to individuals.
24

25 62. In contrast, Sony took very seriously the threat of denial of service
26 attacks on its business, particularly after what had happened to the Sony
27
28

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

3
4 63. In August 2014, a month after Sony settled the class action litigation
5 brought by PlayStation gamers as a result of the April 2011 breach—and just
6 months before the GOP hackers took responsibility for the current Data Breach—
7 hackers again took down the PlayStation Network and also took down Sony’s
8 Entertainment Network by overwhelming Sony’s Network with “denial of service”
9 attacks.
10

11
12 64. Also in August 2014, information technology online publication ARS
13 Technica reported Sony’s Chief Information Security Officer Phil Reitinger
14 announced he would be stepping down, noting that there were a number of archaic
15 systems that had been in place at Sony for ages with plenty of potential attack
16 points.
17

18
19 65. Attacks on Sony’s Network have continued to be reported as recently
20 as December 7, 2014.

21 **E. The Federal Government is Currently Investigating Sony’s Latest Data**
22 **Breach**

23 66. On December 1, 2014, the Federal Bureau of Investigation (“FBI”)
24 launched an investigation into Sony’s cyber-intrusion.
25
26
27
28

1 67. The FBI confirmed on December 8, 2014 that it will advise Sony's
2 employees on how to manage the leak of their personal information in the massive
3 Sony Network Data Breach.
4

5 68. On December 10, 2014, the Senate Committee on Banking, Housing
6 and Urban Affairs held a cybersecurity hearing in which New York Senator
7 Charles Schumer raised concerns over the origin of Sony's current Data Breach.
8

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

11 69. As a result of the Data Breach, cyber-criminals now possess the PII of
12 Sony's current and former employees.
13

14 70. As the Federal Trade Commission has stated, PII such as Social
15 Security numbers, financial information, and other sensitive information are "what
16 thieves use most often to commit fraud or identity theft." In addition, once identity
17 thieves have personal information, "they can drain your bank account, run up your
18 credit cards, open new utility accounts, or get medical treatment on your health
19 insurance."
20

21 71. Legitimate organizations and the criminal underground alike
22 recognize the value of such data. Otherwise, they would not pay for or maintain it,
23 or aggressively seek it. Criminals seek personal and financial information of
24 consumers because they can use biographical data to perpetuate more and larger
25 thefts.
26
27
28

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

3 72. Sony has already acted to protect itself by using hacking methods of
4 its own to combat illegal downloads of its movies that hackers publicly released
5 after the Data Breach, according to Recode. Specifically, it is harnessing Amazon
6 Web Services (the backend that hosts Netflix, Instagram and many others) to
7 launch a distributed denial of service (DDoS) attack on websites hosting the stolen
8 assets.
9

10
11 73. Sony has not, however, similarly acted to protect its current and
12 former employees.
13

14 74. This is important because, according to experts, one out of four data
15 breach notification recipients became a victim of identity fraud, in which an
16 identity thief uses another's personal and financial information such as that
17 person's name, address, and other information, without permission, to commit
18 fraud or other crimes.
19

20 75. For instance, identity thieves may commit various types of crimes
21 such as immigration fraud, obtaining a driver's license or identification card in the
22 victim's name but with another's picture, using the victim's information to obtain
23 government benefits, or filing a fraudulent tax return using the victim's
24 information to obtain a fraudulent refund.
25
26
27
28

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

5
6 77. Furthermore, the PII that Sony failed to adequately protect and that
7 was stolen in the Data Breach is "as good as gold" to identity thieves because
8 identity thieves can use victims' personal data to open new financial accounts and
9 incur charges in another person's name, take out loans in another person's name,
10 and incur charges on existing accounts.

11
12
13 78. Finally, the GOP hackers have already used this PII to harass Sony's
14 employees by threatening harm to their families if they did not cooperate by
15 signing a document evidencing support for the GOP mission and substantially
16 impairing their ability to work while malware was installed on the Sony Network.

17
18 79. The United States government and privacy experts acknowledge that
19 it may take years for identity theft to come to light and be detected.

20
21 80. Accordingly, as Identity Finder LLC CEO Todd Feinman told
22 Law360, the real victims are Sony's employees and ex-employees: "They're now
23 at risk for identity theft for the rest of their lives."

24
25 81. On information and belief, the PII posted to the Internet pertaining to
26 Sony employees was not limited to current employees and dates back to employees
27
28

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

3
4 82. Notably, while several former Sony employees reported seeing their
5 personal data in leaked documents by December 8, 2014, one former high-ranking
6 Sony employee who left the company earlier this year told CNET that: “The
7 studio’s done absolutely nothing to reach out to us.”
8

9 83. On December 9, 2014, on information and belief, Sony began
10 generally responding to inquiries by former Sony employees concerned about the
11 Sony Network Data Breach and public dissemination of former Sony employee PII
12 stolen by the hackers.
13

14 84. Sony’s belated response did not confirm whether specific current or
15 former employees’ PII had been compromised, and instead put the burden on the
16 inquiring current or former employees to act to “minimize your risk of identity
17 theft.” Sony’s response noted that former Sony employees could expect to receive
18 an email within the next several days that would include instructions on how they
19 could sign up for 12 months of identity protection services at no charge with a third
20 party provider of Sony’s choosing.
21
22
23

24 85. In conjunction with its belated disclosure, Sony put the burden on
25 Plaintiffs and the other Class members to monitor for damages caused by the Data
26 Breach, cautioning them to watch out for unauthorized use of their credit card data
27 and identity-theft scams. Implicitly recognizing the damage caused by the Data
28

1 Breach, Sony encouraged Plaintiffs and the other Class members to “remain
2 vigilant, to review your account statements and to monitor your credit reports.”
3

4 86. On December 10, 2014, Twin Cities.com echoed the concern of
5 former Sony employees, reporting that nearly 4,000 people had joined a recently
6 formed Facebook group called “Sony Ex-Employees Worried about the Info
7 Breach,” and that many of those former employees were concerned that they are
8 unable to get information from the studio about how to register for credit
9 monitoring and the identity protection that the studio has now arranged to offer “to
10 all current and potentially affected former employees and their dependents.”
11
12

13 87. On information and belief, on or about December 12, 2014, Sony’s
14 third party identity protection provider AllClear ID began providing former
15 employees with activation codes that they could use to sign up for credit
16 monitoring and an identity theft insurance policy.
17

18 88. Sony’s limited offer of 12 months of credit monitoring and insurance
19 is inadequate. Neither does anything to prevent identity fraud. Credit monitoring
20 only informs a consumer of instances of fraudulent opening of new accounts, not
21 fraudulent use of existing credit cards. Agencies of the federal government and
22 privacy experts acknowledge that stolen data may be held for more than a year
23 before being used to commit identity theft and once stolen data has been sold or
24 posted on the Internet, fraudulent use of stolen data may continue for years.
25
26
27
28

1 92. Plaintiffs also seek to certify a Virginia Subclass consisting of all
2 members of the Class who are residents of Virginia under the respective data
3 breach statute of Virginia set forth in Count IV. This class is defined as follows:
4

5 All former and current employees of Sony who are residents of
6 Virginia whose Personally Identifiable Information was compromised
7 by Sony's security breaches that became public starting in November
8 2014, and any related security breaches.
9

10 93. **Numerosity.** The Class is sufficiently numerous, as approximately
11 15,000 Sony employees and former employees have had their PII compromised.
12 The Putative Class members are so numerous and dispersed throughout the United
13 States that joinder of all members is impracticable. Putative Class members can be
14 identified by records maintained by Defendant.
15
16

17 94. **Common Questions of Fact and Law.** Common questions of fact
18 and law exist as to all members of the Class and predominate over any questions
19 affecting solely individual members of the Class, pursuant to Rule 23(b)(3).
20

21 Among the questions of fact and law that predominate over any individual issues
22 are:
23

24 (1) Whether Sony failed to exercise reasonable care to protect
25 Plaintiffs' and the Class' PII;

26 (2) Whether Sony timely, accurately, and adequately informed
27 Plaintiffs and the Class that their PII had been compromised;
28

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

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

5 (5) Whether Sony was negligent;

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

7 (7) Whether Plaintiffs and the Class are at an increased risk of
8 identity theft as a result of Sony's breaches and failure to protect Plaintiffs'
9 and the Class' PII; and
10

11 (8) Whether Plaintiffs and members of the Class are entitled to the
12 relief sought, including injunctive relief.
13

14
15 95. **Typicality.** Plaintiffs' claims are typical of the claims of members of
16 the Class because Plaintiffs and the Class sustained damages arising out of
17 Defendant's wrongful conduct as detailed herein. Specifically, Plaintiffs' and the
18 Class' claims arise from Sony's failure to install and maintain reasonable security
19 measures to protect Plaintiffs' and the Class's PII, and to timely notify them when
20 the security breach occurred.
21

22 96. **Adequacy.** Plaintiffs will fairly and adequately protect the interests
23 of the Class and has retained counsel competent and experienced in class action
24 lawsuits. Plaintiffs have no interests antagonistic to or in conflict with those of the
25 Class and therefore is an adequate representative for Class.
26
27
28

1 100. Sony owed a duty to Plaintiffs and the members of the Class to
2 provide security, including consistent with of industry standards and requirements,
3 to ensure that its systems and networks, and the personnel responsible for them,
4 adequately protected the PII of its current and former employees.
5

6 101. Sony owed a duty of care to Plaintiffs and the members of the Class
7 because they were foreseeable and probable victims of any inadequate security
8 practices. Sony knew or should have known it had inadequately safeguarded its
9 Network, particularly in light of its multiple prior breaches, as noted above, and yet
10 Sony failed to take reasonable precautions to safeguard current and former
11 employees' PII.
12

13 102. Sony owed a duty to timely and accurately disclose to Plaintiffs and
14 members of the Class that their PII had been or was reasonably believed to have
15 been compromised. Timely disclosure was required, appropriate and necessary so
16 that, among other things, Plaintiffs and the members of the Class could take
17 appropriate measures to avoid identify theft or fraudulent charges, including,
18 monitor their account information and credit reports for fraudulent activity, contact
19 their banks or other financial institutions, obtain credit monitoring services, file
20 reports with law enforcement and other governmental agencies and take other steps
21 to mitigate or ameliorate the damages caused by Sony's misconduct.
22
23

24 103. Plaintiffs and members of the Class entrusted Sony with their PII on
25 the premise and with the understanding that Sony would safeguard their
26
27
28

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

3
4 104. Sony knew, or should have known, of the inherent risks in collecting
5 and storing the PII of Plaintiffs and members of the Class and of the critical
6 importance of providing adequate security of that information.

7
8 105. Sony's own conduct also created a foreseeable risk of harm to
9 Plaintiffs and members of the Class. Sony's misconduct included, but was not
10 limited to, its failure to take the steps and opportunities to prevent and stop the
11 Data Breach as set forth herein. Sony's misconduct also included its decision not to
12 comply with industry standards for the safekeeping and maintenance of the PII of
13 Plaintiffs and members of the Class.

14
15
16 106. Through its acts and omissions described herein, Sony unlawfully
17 breached its duty to use reasonable care to protect and secure Plaintiffs' and the
18 Class' PII within its possession or control. More specifically, Defendant failed to
19 maintain a number of reasonable security procedures and practices designed to
20 protect the PII of Plaintiffs and the Class, including, but not limited to, establishing
21 and maintaining industry-standard systems to safeguard its current and former
22 employees' PII. Given the risk involved and the amount of data at issue, Sony's
23 breach of its duties was entirely unreasonable.
24
25
26
27
28

1 107. Sony breached its duties to timely and accurately disclose that
2 Plaintiffs' and Class members' PII in Sony's possession had been or was
3 reasonably believed to have been, stolen or compromised.
4

5 108. As a direct and proximate result of Defendant's breach of its duties,
6 Plaintiffs and members of the Class have been harmed by the release of their PII,
7 causing them to expend personal income on credit monitoring services and putting
8 them at an increased risk of identity theft. Plaintiffs and members of the Class have
9 spent time and money to protect themselves as a result of Defendant's conduct, and
10 will continue to be required to spend time and money protecting themselves, their
11 identities, their credit, and their reputations.
12
13

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

16 109. Plaintiffs and the Class reallege and incorporate by reference the
17 allegations contained in each of the preceding paragraphs of this Complaint as if
18 fully set forth herein.
19

20 110. California Civil Code § 56, *et seq.*, known as the Confidentiality of
21 Medical Information Act ("Medical Information Act"), requires employers who
22 receive medical information to establish appropriate procedures to ensure the
23 confidentiality and protection from unauthorized use and disclosure of that
24 information. These procedures may include, but are not limited to, instruction
25 regarding confidentiality of employees and agents handling files containing
26
27
28

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

3
4 111. Furthermore, the Medical Information Act prohibits employers from
5 disclosing medical information regarding a patient without first obtaining written
6 authorization from the patient.

7
8 112. In the usual course of business, employers, including Sony, possess
9 and retain certain mediation records and information belonging to its current and
10 former employees, including certain of Plaintiffs' medical information. During
11 their employment with Sony, Plaintiffs lived in California.

12
13 113. At all relevant times, Defendant had a legal duty to protect the
14 confidentiality of Plaintiffs' and Class members' medical information.

15
16 114. By failing to ensure adequate security systems were in place to
17 prevent access and disclosure of Plaintiffs' and Class members' private medical
18 information without written authorization, Defendant violated the Medical
19 Information Act and their legal duty to protect the confidentiality of such
20 information.

21
22 115. Pursuant to Cal. Civ. Code § 56.36, those Plaintiffs and members of
23 the Class whose medical information was compromised are entitled to nominal
24 statutory damages of \$1,000 per class member as well as any actual damages
25 sustained by those Plaintiffs and members of the Class.
26
27
28

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

(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.

* * *

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

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

17 118. The unauthorized acquisition of Plaintiffs’ and Class members’ PII
18 constituted a “breach of the security system” of Sony.
19

20 119. Sony unreasonably delayed informing anyone about the breach of
21 security of California Subclass members’ confidential and non-public information
22 after Sony knew the Data Breach had occurred.
23
24
25
26
27
28

1 125. Plaintiffs and the Class reallege and incorporate by reference the
2 allegations contained in each of the preceding paragraphs of this Complaint as if
3 fully set forth herein.
4

5 126. Section 18.2-186.6 of the Code of Virginia provides, in pertinent part,
6 as follows:
7

8 (B) If unencrypted or unredacted personal information was or is
9 reasonably believed to have been accessed and acquired by an
10 unauthorized person and causes, or the individual or entity reasonably
11 believes has caused or will cause, identity theft or another fraud to any
12 resident of the Commonwealth, an individual or entity that owns or
13 licenses computerized data that includes personal information shall
14 disclose any breach of the security of the system following discovery
15 or notification of the breach of the security of the system to the Office
16 of the Attorney General and any affected resident of the
17 Commonwealth without unreasonable delay. Notice required by this
18 section may be reasonably delayed to allow the individual or entity to
19 determine the scope of the breach of the security of the system and
20 restore the reasonable integrity of the system. Notice required by this
21 section may be delayed if, after the individual or entity notifies a law-
22 enforcement agency, the law-enforcement agency determines and
23 advises the individual or entity that the notice will impede a criminal
24
25
26
27
28

1 or civil investigation, or homeland or national security. Notice shall be
2 made without unreasonable delay after the law-enforcement agency
3 determines that the notification will no longer impede the
4 investigation or jeopardize national or homeland security.
5

6 (C) An individual or entity shall disclose the breach of the security of
7 the system if encrypted information is accessed and acquired in an
8 unencrypted form, or if the security breach involves a person with
9 access to the encryption key and the individual or entity reasonably
10 believes that such a breach has caused or will cause identity theft or
11 other fraud to any resident of the Commonwealth.
12

13 (D) An individual or entity that maintains computerized data that
14 includes personal information that the individual or entity does not
15 own or license shall notify the owner or licensee of the information of
16 any breach of the security of the system without unreasonable delay
17 following discovery of the breach of the security of the system, if the
18 personal information was accessed and acquired by an unauthorized
19 person or the individual or entity reasonably believes the personal
20 information was accessed and acquired by an unauthorized person.
21

22 (E) In the event an individual or entity provides notice to more than
23 1,000 persons at one time pursuant to this section, the individual or
24 entity shall notify, without unreasonable delay, the Office of the
25
26
27
28

1 Attorney General and all consumer reporting agencies that compile
2 and maintain files on consumers on a nationwide basis, as defined in
3 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the
4 notice.
5

6 127. For purposes of this section, “personal information” means the first
7 name or first initial and last name in combination with and linked to any one or
8 more of the following data elements that relate to a resident of the Commonwealth,
9 when the data elements are neither encrypted nor redacted:
10

11 (a) Social security number;

12 (b) Driver’s license number or state identification card number issued
13 in lieu of a driver’s license number; or
14

15 (c) Financial account number, or credit or debit card number, in
16 combination with any required security code, access code, or
17 password that would permit access to a resident’s financial account.
18

19 128. For purposes of this section, “notice” means:
20

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

23 (2) Telephone notice;

24 (3) Electronic notice; or
25

26 (4) Substitute notice, if the individual or the entity required to provide notice
27 demonstrates that the cost of providing notice will exceed \$50,000, the
28

1 affected class of Virginia residents to be notified exceeds 100,000 residents,
2 or the individual or the entity does not have sufficient contact information or
3 consent to provide notice as described in subdivisions 1, 2, or 3 of this
4 definition. Substitute notice consists of all of the following:
5

6 (a) E-mail notice if the individual or the entity has e-mail addresses
7 for the members of the affected class of residents;
8

9 (b) Conspicuous posting of the notice on the website of the
10 individual or the entity if the individual or the entity maintains a website;
11 and
12

13 (c) Notice to major statewide media.

14 129. Further, the “notice” required by this section shall include a
15 description of the following:
16

17 (1) The incident in general terms;

18 (2) The type of personal information that was subject to the unauthorized
19 access and acquisition;
20

21 (3) The general acts of the individual or entity to protect the personal
22 information from further unauthorized access;
23

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

26 (5) Advice that directs the person to remain vigilant by reviewing account
27 statements and monitoring free credit reports.
28

1 130. “Breach of the security of the system” means the unauthorized access
2 and acquisition of unencrypted and unredacted computerized data that
3
4 compromises the security or confidentiality of personal information maintained by
5 an individual or entity as part of a database of personal information regarding
6 multiple individuals and that causes, or the individual or entity reasonably believes
7 has caused, or will cause, identity theft or other fraud to any resident of the
8 Commonwealth. Good faith acquisition of personal information by an employee or
9 agent of an individual or entity for the purposes of the individual or entity is not a
10 breach of the security of the system, provided that the personal information is not
11 used for a purpose other than a lawful purpose of the individual or entity or subject
12 to further unauthorized disclosure.
13
14

15
16 131. The unauthorized acquisition of Plaintiffs’ and Class members’ PII
17 constituted a “breach of the security of the system” of Sony under Section 18.2-
18 186.6.A. of the Code of Virginia.
19

20 132. Sony unreasonably delayed informing anyone about the breach of
21 security of Virginia Subclass members’ confidential and non-public information
22 after Sony knew the Data Breach had occurred.
23

24 133. Defendant failed to disclose to Virginia Subclass members, without
25 unreasonable delay, and in the most expedient time possible, the breach of security
26 of their unencrypted, or not properly and securely encrypted, personal information
27 when they knew or reasonably believed such information had been compromised.
28

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

3
4 B. Finding that Sony breached its duty to safeguard and protect
5 Plaintiffs' and the Class' PII that was compromised in the security breach that
6 became public knowledge starting in November 2014;

7
8 C. That the Court award Plaintiffs and the Class appropriate relief,
9 including any actual and statutory damages, restitution and disgorgement.

10 D. That the Court award equitable, injunctive and declaratory relief as
11 may be appropriate under applicable state laws. Plaintiffs, on behalf of the Class
12 seeks appropriate injunctive relief, including but not limited to: (i) the provision of
13 credit monitoring and/or credit card monitoring services for the Class for at least
14 five years; (ii) the provision of bank monitoring and/or bank monitoring services
15 for the Class for at least five years; (iii) the provision of identity theft insurance for
16 the Class for at least five years; (iv) the provision of credit restoration services for
17 the Class for at least five years; (v) awarding Plaintiffs and the Class the
18 reasonable costs and expenses of suit, including attorneys' fees, filing fees, and
19 insurance for the Class; and (vi) requiring that Sony receive periodic compliance
20 audits by a third party regarding the security of its computer systems used for
21 storing current and former employee data, to ensure against the recurrence of a
22 data breach by adopting and implementing best security data practices;
23
24
25
26
27

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

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

3
4 G. Awarding pre-judgment and post-judgment interest as prescribed by
5 law; and

6 H. Granting additional legal or equitable relief as this Court may find just
7 and proper.
8

9 **JURY TRIAL DEMANDED**

10 Plaintiffs hereby demand a trial by jury on all issues so triable.
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 DATED this 15th day of December, 2014.

2 **KELLER ROHRBACK L.L.P.**

3 By s/ Khesraw Karmand

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

11 Lynn Lincoln Sarko, *pro hac vice*
12 *forthcoming*

13 lsarko@kellerrohrback.com

14 Gretchen Freeman Cappio, *pro hac vice*
15 *forthcoming*

16 gcappio@kellerrohrback.com

17 Cari Campen Laufenberg, *pro hac vice*
18 *forthcoming*

19 claufenberg@kellerrohrback.com

20 Amy N.L. Hanson, *pro hac vice forthcoming*
21 ahanson@kellerrohrbak.com

22 1201 Third Ave., Suite 3200

23 Seattle, Washington 98101

24 Tel: (206) 623-1900 / Fax: (206) 623-3384

25 ***Attorneys for Plaintiffs Michael Corona***
26 ***and Christina Mathis***