Matthew J. Preusch (SBN 298144)
mpreusch@kellerrohrback.com
KELLER ROHRBACK L.L.P.
1129 State Street, Suite 8
Santa Barbara, CA 93101
T: (805) 456-1496
F: (805) 456-1497

Lynn Lincoln Sarko, *admitted pro hac vice*
lsarko@kellerrohrback.com
KELLER ROHRBACK L.L.P
1201 Third Avenue, Suite 3200
Seattle, WA 98101
T: (206) 623-1900
F: (206) 623-3384
Attorneys for Plaintiffs Michael Corona and Christina Mathis

Daniel C. Girard (SBN 114826)
dcg@girardgibbs.com
GIRARD GIBBS LLP
601 California Street, 14th Floor
San Francisco, CA 94108
T: (415) 981-4800
F: (415) 981-4846
Attorneys for Plaintiffs Joshua Forster and Ella Carline Archibeque

Michael W. Sobol (SBN 194857)
msobol@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
T: (415) 956-1000
F: (415) 956-1008
Attorneys for Plaintiffs Michael Levine and Geoffrey Springer

Additional Counsel listed below

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

MICHAEL CORONA, CHRISTINA MATHIS, et al., individually and on behalf of others similarly situated,

Plaintiffs,

vs.

SONY PICTURES ENTERTAINMENT, INC.,

Defendant.

CASE NO. 2:14−CV−09600−RGK−SH

CLASS ACTION

AMENDED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Raúl Pérez
Raul.Perez@Capstonelawyers.com
CAPSTONE LAW APC
1840 Century Park East, Suite 450
Los Angeles, CA 90067
T: (310) 556-4811
F: (310) 943-0396
Attorneys for Plaintiff Marcela Bailey

John H. Gomez
john@gomeztrialattorneys.com
GOMEZ TRIAL ATTORNEYS
655 West Broadway, Suite 1700
San Diego, CA 92101
T: (619) 237-3490
F: (619) 237-3496
Attorneys for Plaintiffs Steven Shapiro and Lawon Exum

Steven M. Tindall
stindall@rhdtlaw.com
RUKIN HYLAND DORIA & TINDALL LLP
100 Pine Street, Suite 2150
San Francisco, CA 94111
T: (415) 421-1800
F: (415) 421-1700

TABLE OF CONTENTS

Page

I. INTRODUCTION

Plaintiffs Michael Corona, Christina Mathis, Joshua Forster, Ella Carline Archibeque, Michael Levine, Geoffrey Springer, Marcela Bailey, Steven Shapiro, and Lawon Exum ("Plaintiffs"), individually and on behalf of all others similarly situated, file this Amended Class Action Complaint against Sony Pictures Entertainment, Inc. ("Defendant" or "SPE"), and allege as follows based on personal knowledge, the investigation of their counsel, and information and belief.

II. NATURE OF THE ACTION

1. An epic nightmare, much better suited to a cinematic thriller than to real life, has been unfolding in slow motion for thousands of current and former employees of SPE. In late November and December 2014, they learned that they were the victims of a massive data breach first publicized by the media in late November 2014 (the "Data Breach") that resulted in the posting of SPE's personnel records on the internet. The Data Breach resulted in the public disclosure of employees' most sensitive, non-public personal identifying information ("PII"), including Social Security numbers, employment files, salary and bank account information, health insurance and other medical information, their names, home and email addresses, visa and passport numbers, and retirement plan data, as well as their family members' similar information. These records were and are posted on file-sharing websites for identity thieves to download, have been published in news

reports, and were used to send emails threatening physical harm to employees and their families.[1]

2. Cybercriminals were able to perpetrate a breach of this depth and scope because SPE failed to maintain reasonable and adequate security measures to protect the employees' information from access and disclosure. SPE has obligations, by statute and otherwise, to protect its employees' employment and personnel records from unauthorized access, yet failed at numerous opportunities to prevent, detect, end, or limit the scope of the breach. Among other things, (1) SPE failed to implement security measures designed to prevent this attack even though there have been similar cyber-attacks of SPE and its sister companies; (2) SPE failed to employ security protocols to detect the breach and removal of nearly 100 terabytes of data from its computer networks; and (3) SPE failed to maintain basic security measures such as access controls and requiring passwords with appropriate levels of complexity and encryption, measures that would have ensured that data would be

[1] As Plaintiffs have represented to the Court, simultaneously with the filing of this Amended Class Action Complaint, Plaintiffs in the following actions are filing notices of voluntary dismissal without prejudice filed under Fed. R. Civ. P. 41, and will proceed as named plaintiffs or proposed class members in this action:

- *Forster et al. v. Sony Pictures Entertainment, Inc.*, No. 2:14-cv-09646-RGK-SH
- *Levine et al. v. Sony Pictures Entertainment, Inc.*, No. 2:14-cv-09687-RGK-SH
- *Bailey v. Sony Pictures Entertainment, Inc.*, No. 2:14-cv-09755-RGK-SH
- *Shapiro v. Sony Pictures Entertainment, Inc.*, No. 2:14-cv-09762-RGK-SH
- *Rodriguez v. Sony Pictures Entertainment, Inc.*, No. 2:15-cv-00014-RGK-SH
- *Exum v. Sony Pictures Entertainment, Inc.*, No. 2:15-cv-00111-CAS-RGK-SH

harder to access or steal and, in the event data were accessed or stolen, it would be unreadable and thus cause less damage to SPE employees and their families.

3. Following the breach, SPE has focused on its own remediation efforts, *not* on protecting its employees' sensitive records or minimizing the harm to its employees and their families. Rather, SPE has focused on securing its own intellectual property from pirates and a public relations campaign directed at controlling the damage to SPE associated with the release of embarrassing internal emails. Meanwhile, SPE delayed confirming the Data Breach and left its employees in the dark about the scope of the breach, how they and their families were impacted, and what steps SPE is taking to remedy or mitigate the breach. Due to SPE's delay, current and former SPE employees have purchased identity protection services and insurance and taken other measures to protect their compromised PII, yet remain vulnerable to identity theft, medical identity theft, tax fraud, and financial theft because their Social Security numbers, financial information and medical information have been, and may still be, publicly available to anyone with an internet connection. SPE's conduct is a direct cause of the ongoing harm employees are currently suffering and will continue to experience for the indefinite future.

4. Plaintiffs are former SPE employees who bring this proposed class action lawsuit on behalf of employees whose PII has been compromised as a result of the Data Breach. Plaintiffs and class members, as well as their family members, will have to remain vigilant for the rest of their lives to combat potential identity theft

arising from the staggering amount of financial, medical and other personal information that is not only in the hands of cyber criminals, but that has also been posted on the internet for anyone to gather and use for any purpose, at any time, in perpetuity. Despite all best efforts of Plaintiffs, class members, or anyone else, this most sensitive personal data can never be made private again.

5. Plaintiffs allege that SPE failed to adequately safeguard its current and former employees' PII, including Social Security numbers, medical records, and financial information, in compliance with applicable law. Plaintiffs seek injunctive relief requiring SPE to implement and maintain security practices to comply with regulations designed to prevent and remedy these types of breaches, as well as restitution, damages, and other relief.

III. JURISDICTION

6. This Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because the amount in controversy exceeds $5 million, exclusive of interest and costs, and members of the proposed class are citizens of different states than Defendant SPE.

7. This Court has personal jurisdiction over SPE because SPE maintains its headquarters in California, is registered to conduct business in California, and has sufficient minimum contacts with California.

8. Venue is proper in this district under 28 U.S.C. § 1391(b) because SPE resides in this district and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this district.

IV. PARTIES

9. Plaintiff Michael Corona is a resident of Virginia.

10. Plaintiff Christina Mathis is a resident of California

11. Plaintiff Joshua Forster is a resident of Colorado.

12. Plaintiff Ella Carline Archibeque is a resident of California.

13. Plaintiff Michael Levine is a resident of California.

14. Plaintiff Geoffrey Springer is a resident of Virginia.

15. Plaintiff Marcela Bailey is a resident of California.

16. Plaintiff Steven Shapiro is a resident of California.

17. Plaintiff Lawon Exum is a resident of California.

18. Each Plaintiff had sensitive, non-public information compromised due to the Data Breach and has been injured as a result.

19. Defendant Sony Pictures Entertainment, Inc. is a corporation organized under the laws of Delaware with its principal place of business in Culver City, California.

V. FACTUAL ALLEGATIONS

A. The Data Breach Exposed the Financial, Medical and Other Personal Information of SPE's Current and Former Employees

20. On November 24, 2014, the media reported that SPE was subject to an undetected data breach whereby nearly 100 terabytes of data was seized from the company and caused the leak of the financial, medical, and other personal information of thousands of current and former employees on the internet.

21. A hacker group calling itself the Guardians of Peace, or "#GOP", took over SPE's network, displayed its own messages and an image of a skeleton, seized control of promotional Twitter accounts for SPE movies, and warned SPE that it had obtained "secrets" that it threatened to leak on the Web:

22. The hackers began releasing portions of stolen data to the public on November 30, 2014, beginning with a series of unreleased movies produced by SPE. The media then reported receiving emails with links to a file on Pastebin, a file-sharing site that contained a trove of SPE employees' personnel information.

23. Security researcher Brian Krebs, who was the first to uncover many of the recent high-profile data breaches at companies like Target Corporation and The Home Depot, reported in a December 2, 2014 blog post that several of his sources had confirmed that the hackers had stolen more than 25 gigabytes of sensitive data, including Social Security numbers and medical and salary information, of tens of thousands of current and former SPE employees.

24. Mr. Krebs reported that he had observed files being traded on torrent networks, including a global employee list containing names, employee IDs, usernames, and birthdates of current and former SPE employees, and a list containing names, birthdates, Social Security numbers and health savings account data. The files included a Microsoft Excel document with the name, location, employee ID, network username, base salary and date of birth of more than 6,800 employees; a status report from April 2014 listing the names, dates of birth, Social Security numbers and health savings account data of more than 700 employees; and a file that appeared to be part of an internal audit report from PricewaterhouseCoopers, made up of screen shots of dozens of employees' federal tax records and other compensation data. Mr. Krebs found that a "comprehensive search on LinkedIn for dozens of names in the [Microsoft Excel] list indicate[d] that virtually all correspond to current or former Sony employees."

25. Kevin Roose, a well-regarded technology writer, reported that the initial leak also included a spreadsheet listing the names, birth dates, and Social Security

numbers of 3,803 SPE employees; a spreadsheet listing the division-by-division SPE payroll, as well as costs for raises and other pay changes; a spreadsheet listing SPE employees who were fired or laid off in 2014 as part of the company's reorganization, along with the reasons for their terminations and the estimated costs for severance pay, COBRA health benefits, and outplacement costs; and detailed performance reviews for hundreds of SPE employees.

26. On December 5, 2014, sources reported that the Data Breach had exposed even more personal information than had been previously reported, including over 47,000 unique Social Security numbers, more than 15,200 of which belong to current and former SPE employees. Some of these employees were last employed by SPE as long ago as 1955, raising concerns about SPE's data retention policies. The Social Security numbers were copied more than 1.1 million times throughout the 601 files stolen by hackers according to Identity Finder LLC, which analyzed the breached data. This personal information was found in more than 500 spreadsheets, 75 PDFs, and several Microsoft Word documents, none of which were protected by passwords. As Identity Finder CEO Todd Feinman explained, 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 posted online on multiple file-sharing websites.

27. Hackers also used the stolen data to threaten SPE's employees and their families with physical harm. On December 5, 2014, many current and former SPE

employees received an email in which they were told: "[p]lease 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."

28. As of December 8, 2014, hackers had released around 140 gigabytes of a cache of internal SPE files and films they claimed totals around 100 terabytes—approximately ten times the amount of information stored in the Library of Congress. Two days later, the hackers posted additional data with a message to SPE employees threatening to release even more of their sensitive personal information:

> SPE Employees!
>
> Don't believe what the executives of SPE says.
>
> They say as if the FBI could resolve everything.
>
> But the FBI cannot find us because we know everything about what's going on inside the FBI.
>
> We still have huge amount of sensitive information to be released including your personal details and mailboxes.
>
> If continued wrongdoings of the executives of SPE drive us to make an unwanted decision, only SPE should be blamed.
>
> Now is the time for you to choose what to do.
>
> We have already given much time for you.

29. The hackers posted an estimated 38 million files on file-sharing sites in eight separate leaks, consisting of massive amounts of SPE employee data in addition to internal SPE emails, profit-and-loss statements, and scripts for upcoming SPE television shows and movies. The leaked employee data included names, employee

IDs, dates of birth, home addresses, Social Security numbers, copies of passports and visas, job titles, salaries and bonus information, tax records, employment contracts, information regarding employee benefits, medical plans, dental plans, workers compensation details, retirement and termination plans, receipts for travel, prior work history, performance reviews, criminal background checks, and details of severance packages.

30. The leaks also included SPE employees' medical information, and the medical information of their family members. For example, one memo from a human resources executive to the company's benefits committee disclosed details of an employee's child with special needs, including the child's name, diagnosis and details of the child's treatment. The leaked data also includes emails between SPE's insurance company and its human resources department about the surgery of a named employee's spouse and another employee's claim for speech therapy lessons. Another leaked document was a spreadsheet from a human resources folder that includes the birth dates, gender, health condition, and medical costs for 34 SPE employees, their spouses and children. The listed conditions include premature births, cancer, kidney failure and alcoholic liver cirrhosis, though not the employees' names. Even without the names, however, the document's inclusion of "member keys" and birth dates could allow someone with access to other employee documents to identify the employees. Another leaked document listed the Social Security numbers, insurance policy numbers, names, birth dates and addresses for more than

100 employees. Several other leaked documents detailing overpayments made by Aetna contained insurance claim numbers, member identification numbers, and the names of employees.

B. Successive Data Breaches at SPE[2] and Other Sony Companies Exposed Data Security Weaknesses

31. SPE has been a longstanding and frequent target for hackers, but it apparently made a conscious and deliberate business decision to accept both the risk of losses and the actual losses associated with being hacked.

32. SPE's sister companies, Sony Network Entertainment International LLC and Sony Computer Entertainment America LLC, experienced massive data breaches in April 2011, which compromised information from approximately 101 million users accounts, including 12 million unencrypted credit card numbers. Two weeks before those breaches, the companies received an anonymous warning:

> 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.

33. One of the 2011 data breaches involved Sony's PlayStation® Network ("PSN"). After the data breach became public, it became clear that while the Sony companies invested significant resources in protecting their own confidential

[2] SPE is an indirect, wholly owned subsidiary of Sony Corporation of America ("Sony America"), which is a wholly owned, indirect subsidiary of Sony Corporation ("Sony").

proprietary information, they failed to establish even the most basic safeguards for the PSN and its consumer data. Among other things, the PSN was not protected by appropriate firewalls, a deviation from widespread industry practice and standards. As a result, hackers were able to steal the personal information associated with all of the approximately 77 million customer accounts. Experts have attributed the PSN breach to an unsophisticated method of hacking that would not have been successful if even the most basic security measures had been in place.

34. PSN users filed class action cases after the 2011 breach, which Sony agreed to settle in June 2014 in exchange for $15 million in games, online currency, and identity theft reimbursement.

35. Following the PSN breach, Shinji Hasejima, Chief Information Officer of SPE's parent Sony, admitted that the attack exploited a "known vulnerability" in the application server platform used in the PSN. Sony President Kazuo Hirai admitted that the company's security had been inadequate before the attack, saying that after the hack, the company had "basically … done everything to bring our practices at least in line with industry standards or better."

36. Despite these public statements that the company had corrected its inadequate security measures, Sony's networks remained highly vulnerable to attack. John Bumgarner, the chief technology officer of the United States Cyber-Consequences Unit, uncovered numerous security problems on company webpages

that were readily accessible. He discovered that unauthorized users could still access internal Sony resources, including security management tools.

37. In June 2011, SPE itself experienced a data breach in which hackers stole the personal data of over one million customers and released more than 150,000 of the stolen records. The stolen data included names, home addresses, birthdates, email addresses, and phone numbers, as well as customer passwords, which were stored unencrypted.

38. Following the 2011 data breaches, PCWorld technology journalist Tony Bradley observed that Sony "seems to ignore compliance requirements and basic security best practices, so it is basically begging to be attacked." He advised companies to follow security "best practices and data security compliance requirements"—and in short—"Don't be a Sony." Fred Touchette of email and web security firm AppRiver echoed Bradley's comments, saying, "There 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."

39. Sony's security gaps, and the attacks, continued. In 2013, hackers infiltrated Sony's network, stole gigabytes of data several times a week and encrypted the information to cover their tracks.

40. In February 2014, hackers accessed an FTP server used in connection with SPE's international theatrical sales and distribution system, SpiritWorld. The

login credentials for two user accounts were compromised and the personal data of 759 individuals associated with theaters in Brazil, along with payment information for Brazil film distributors, was stolen. SPE had been storing the payment information as .txt files since 2008.

41. In August 2014, approximately one month after Sony settled the class action litigation brought by PlayStation® gamers as a result of the April 2011 breach—and just three months before the Data Breach at SPE— hackers again took down the PSN as well as the Sony Entertainment Network via "denial of service" attacks. The hackers posted on Twitter that their attacks were intended to raise awareness of Sony's inadequate security measures.

C. Ignoring Prior Data Breaches and the Warnings of Its Employees and Third-Party Auditors, SPE Favored Cost Savings and Convenience Over Sound Data Security Principles

42. Given the recent increase of data breaches aimed at major corporations and the prior data breaches at SPE and its sister companies, one would expect that SPE would be more vigilant than ever regarding the need to adopt, implement, and maintain security measures to protect its confidential data, including its employees' PII. Instead, SPE has emphasized cost savings over compliance when it comes to data security.

43. The technology and business website CIO reported that a 2005 audit of SPE's security practices alerted Jason Spaltro, SPE's executive director of information security, to several security weaknesses in the company's systems,

including insufficiently strong access controls, a key Sarbanes-Oxley requirement. In a 2007 interview, Mr. Spaltro was interviewed about compliance with security and privacy regulations. Discussing the risk analysis of protecting private data, he weighed the hypothetical $10 million cost of preventing a potential intrusion against the hypothetical $1 million cost of responding to a breach. "With those numbers, says Spaltro, 'it's a valid business decision to accept the risk' of a security breach. 'I will not invest $10 million to avoid a possible $1 million loss,' he suggests."

44. Ari Schwartz, a privacy expert at the Center for Democracy and Technology, called Spaltro's reasoning "shortsighted" because the cost of notification is only a small part of the potential cost to a company. Indeed, Sony reported that the 2011 PSN data breach cost the company $170 million.

45. On information and belief, in 2011, SPE tasked a group of employees to conduct an assessment of the company's data security practices. The assessment was designed to: (1) identify vulnerable data—referred to as "IT assets"—that would be embarrassing if compromised and made publicly available; (2) identify existing security gaps with regard to protecting the implicated IT assets; and (3) recommend steps that could be taken to eliminate these security gaps.

46. The project was conducted over two months in 2011, and one of the principal IT assets identified by the group was a series of databases containing employee PII. Specifically, the group found that human resources records containing employees' PII were unencrypted ("cleartext") and were universally accessible on

SPE's network. The group recommended, among other things, that the identified databases be both encrypted and segregated from the rest of SPE's network (with access being as limited as possible). These recommendations—as well as the identification of the databases and their vulnerabilities—were incorporated into a final report, which took the form of a PowerPoint presentation sent to Mr. Spaltro and SPE CIO Steven Andajar. SPE declined to adopt its own security recommendations, as evidenced by the fact that employee PII was stolen, in unencrypted form, in the Data Breach.

47. Nevertheless, Lockheed Martin security researchers notably publicized in March 2011 a cyberattack kill chain process, which was developed as a response to a new, sophisticated type of hacking called advanced persistent threats ("APTs") that were bypassing traditional static cyber security tools and allowing information security professionals to proactively remediate and mitigate targeted, coordinated, purposeful, and persistent future cyber threats. The kill chain takes advantage of the seven steps a hacker must take to plan and execute a successful attack and allows companies to thwart the APT cyberattack by stopping the hacker from completing *just one* of these seven required steps. In other words, a company has several different opportunities along the kill chain to thwart an attack.

48. In 2013, reports from the United States government and several private security research firms widely distributed reports about new types of malicious

computer code that should have put SPE on notice that cyber-attacks on retailers continued to evolve.

49. Nevertheless, SPE's security practices continued to fall below not only prudent industry standards for prevention, detection, and/or containment of APT hacking, but also traditional, static cyber-attack security standards.

50. On information and belief, between 2013 and 2014, a project was undertaken to migrate 10 million SPE documents from one database called Stellent to another called Al Fresco. The migration included payroll information and other sensitive PII. None of the data in the Stellent database was encrypted. And less than one third of the data was encrypted after it was migrated to Al Fresco. SPE deliberately chose to leave the data unencrypted for the sake of convenience (encrypted information is not searchable), despite the risks it posed to the security of important and sensitive PII.

51. SPE's security practices continue to fall below prudent industry standards. Kevin Roose reported that SPE took a "remarkably lax approach to data security," given that some of the files released in the Data Breach that contained personal employee data were "unencrypted Excel and Word files, labeled plain as day." Time Magazine reported a former employee's criticism of SPE's information security team and that SPE largely ignored the employees' reports of security violations: "Sony's 'information security' team is a complete joke. We'd report security violations to them and our repeated reports were ignored." SPE also

dedicated insufficient resources to data security. The leaked documents show that out of 7,000 employees, only eleven were assigned to the information security team, far too few for a multi-billion dollar company with vast amounts of confidential data.

52. Just two months before the Data Breach became public, on September 25, 2014, PricewaterhouseCoopers delivered a report of its audit of SPE's computer network. The report detailed gaps in the company's monitoring of its systems, including a firewall and more than 100 other devices that were not being monitored by the corporate security team in charge of overseeing infrastructure. The auditors found that SPE had failed to notify the corporate security team of newly added devices to monitor, including web servers and routers. PricewaterhouseCoopers warned that "[s]ecurity incidents impacting these network or infrastructure devices may not be detected or resolved timely." The report concluded that SPE "was failing to monitor 149 out of a final total of 869 systems they wished to monitor. That meant they were blind to 17 percent of their environment."

53. The leaked emails also exposed lax security practices, including CEO Michael Lynton "routinely receiv[ing] copies of his passwords in unsecure emails for his and his family's mail, banking, travel and shopping accounts, from his executive assistant, David Diamond." A leaked email from October 2014 reveals additional problems with SPE's computer system. David C. Hendler, SPE's CFO, complained that the company had experienced months of "significant and repeated outages due to a lack of hardware capacity, running out of disk space, software patches that

impacted the stability of the environment, poor system monitoring and an unskilled support team."

54. SPE has also failed to vigilantly employ intrusion prevention and detection protocols that would have prevented and immediately detected the breach in November 2014. Some experts who have analyzed the malicious software behind the Data Breach have suggested that the hackers may have been inside SPE's network for some time, allowing them to become familiar with the network.

55. Several security firms have noted that the data released by the hackers included a number of SPE'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." A hacker who has access to the cryptographic keys can access encrypted servers without triggering intrusion detection systems because these systems assume the encrypted data is safe. 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 are known to be vulnerable. Mr. Bocek noted that the 2011 PSN breach also compromised cryptographic keys, raising the question of why the Sony companies hadn't established greater protection for them by 2014.

56. Anyone with access to the cryptographic keys could access SPE's network until the company changed them—a process made more difficult by the fact

that Sony apparently did not appropriately track the ways that cryptographic keys are used. For example, Kaspersky Lab pointed out that a sample of the malware that hackers installed on the SPE network during the Data Breach showed traces of being signed by a valid digital certificate from SPE. 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.

57. SPE's ability to prevent further unauthorized access to its network has been severely compromised given the hacker's access to and ability to release the cryptographic keys. In addition, ARS Technica reported that the hackers were able to collect significant intelligence on the network from SPE's own information technology department, including lists of all computers on SPE's internal networks. Among 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 SPE's Information Systems Service (ISS) infrastructure. 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 SPE's network offline as part of the Data Breach.

58. Leaked emails from SPE's general counsel and chief compliance officer, Leah Weil, provided additional insight into SPE's deficient security practices. Among other topics, the emails voiced concerns about the volume of data available

on emails and SPE's email retention policies. For example, one of Ms. Weil's emails reportedly stated, "[w]hile 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."

59. SPE has claimed that the Data Breach was "unprecedented in nature" and "undetectable by industry standard antivirus software." The actual details tell a very different story. As Adam Caudill, an independent security researcher, suggests, "[t]o protect their image, [SPE] need[s] this to be an unpreventable, incredibly sophisticated attack." But the hackers' ongoing conduct should not have remained undetected, he explains: "Even if they couldn't detect the malware, they should have detected the unusual activity. You don't steal such a large amount of data without raising some red flags—the question is, was anyone watching?"

60. Mike Gillepsie of Computer Weekly noted that "[t]his was a sustained attack of various visits and Sony was not aware until it was pointed out, and that is worth discussing." He added, "[o]nce the attackers had found their way in, they took time to build a picture of the network architecture and then returned at a future point to attack specific servers—stealing information and then deleting the original files with sophisticated malware." Mr. Gillepsie pointed out that a major security issue the Data Breach exposed was the lack of "effective segregation of data," a problem that "seems to be across the corporation as the hackers were able to easily move between

areas, taking whatever they picked. … The lack of segregation of data is a very poor security hygiene and given the details released by the hackers of usernames and passwords, this was not the only neglected area of security hygiene at Sony." It is not yet known how the hackers actually breached the network, "but once inside, Sony certainly made it easy for them to move around and take what they wanted with impunity." Philip Lieberman, the president of security management firm Lieberman Software, said: "It's obvious from the scope of what's been done that the intruders owned the entire environment . … Sony lost control of their environment."

D. Current and Former SPE Employees Are Victims of the Breach

61. In addition to implementing a sophisticated public relations campaign to portray the breach as beyond its control, SPE focused its early remediation efforts, *not* on protecting its employees and their families affected by the Data Breach, but rather on controlling the damage associated with unflattering comments in emails about movie stars and politicians and removing pirated films from the internet. SPE used hacking methods of its own to combat illegal downloads of its movies that the hackers publicly released.

62. Meanwhile, SPE failed to provide its current and former employees with concrete information about the breach, what data was exposed, and how SPE will protect their information going forward. Employees who called and emailed SPE were routinely ignored or given rote and unhelpful responses. One employee said,

"We got more information from blogs and websites than we did from Michael [Lynton, CEO of SPE] and Amy [Pascal, co-chair of SPE]."

63. It was not until the evening of December 2, 2014—more than a week after the breach was revealed—that SPE finally issued an official internal memo to 6,500 employees confirming that the Data Breach was authentic, and "that a large amount of confidential Sony Pictures Entertainment data has been stolen by the cyber attackers, including personnel information and business documents." SPE advised employees "to assume that information about you in the possession of the company might be in [the hackers'] possession."

64. SPE sent a second company-wide memo to employees on December 8, assuring them that SPE was doing everything it could to protect them, stating that the FBI has "dedicated their senior staff to this global investigation" and that "recognized experts are working on this matter and looking out for our security."

65. In another memo to employees about the Data Breach dated December 8, 2014, SPE advised that it "believes that the following types of personally identifiable information that you provided to SPE may have been obtained by unauthorized individuals: (i) name, (ii) address, (iii) Social Security number, driver's license number, passport number, and/or other government identifier, (iv) bank account information, (v) credit card information for corporate travel and expense, (vi) username and passwords, (vii) compensation and (viii) other employment related information. In addition, unauthorized individuals may have obtained (ix) HIPAA

protected health information, such as name, Social Security number, claims appeals information you submitted to SPE (including diagnosis and disability code), date of birth, home address, and member ID number to the extent that you and/or your dependents participated in SPE health plans, and (x) health/medical information that you provided to us outside of SPE health plans." SPE warned its employees "to be especially aware of email, telephone, and postal mail scams that ask for personal or sensitive information" and "to remain vigilant, review your account statements, monitor your credit reports and change your passwords" to "protect against possible identity theft or other financial loss."

66. SPE has yet to notify all of its former employees about the breach and the extent of their data that was exposed. While several former SPE employees reported seeing their personal data in leaked documents by December 8, 2014, one former high-ranking employee who left the company earlier in the year told CNET that "[t]he studio's done absolutely nothing to reach out to us."

67. SPE posted a "message" for current and former employees on its website on December 15, 2014 advising that "the security of certain personally identifiable information about its current and former employees, and their dependents that participated in SPE health plans and other benefits, may have been compromised." SPE said that it "has continued to engage in an effort to reach out to potentially impacted individuals with notification about this situation." SPE later sent this message to some, but not all, former employees.

68. As a result of SPE's negligent security practices and slow response to the breach, SPE's current and former employees and their family members are subject to an increased and concrete risk of identity theft due to the exposure of their financial, medical and other personal information and they have spent and will have to continue to spend substantial time and money securing their personal information and accounts and protecting their identities.

69. An identity thief uses another's personal and financial information, such as the person's name, address, and other information, without permission, to commit fraud or other crimes. Identity thieves may commit various types of crimes, from immigration fraud, obtaining a driver's license or identification card in the victim's name, using the victim's information to obtain government benefits, to filing a fraudulent tax return using the victim's information to obtain a refund. Identity thieves may also obtain medical services using stolen medical data or commit any number of other frauds, such as obtaining a job, procuring housing or even giving false information to police during an arrest. They can also use victims' personal information 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.

70. There is a strong likelihood that current and former SPE employees, as well as their family members, are already or will become victims of identity fraud given the breadth of information about them that is now publicly available. Javelin

Strategy & Research reported in its 2014 Identity Fraud Study that "[d]ata breaches are the greatest risk factor for identity fraud." In fact, "[i]n 2013, one in three consumers who received notification of a data breach became a victim of fraud." Javelin also found increased instances of fraud other than credit card fraud, including "compromised lines of credit, internet accounts (e.g., eBay, Amazon) and email payment accounts such as PayPal."

71. As SPE itself recommended, current and former SPE employees and their family members will have to monitor their accounts and credit, and will also have to pay for credit monitoring or credit reports to make sure their credit and identity is not harmed by thieves. Individuals whose bank information was compromised may have to pay fees to their banks for new debit and credit cards, or have to pay fees to have the cards shipped faster so that they do not have to wait weeks to make purchases on their accounts. These individuals may also lose access to their funds and time and money by spending hours on the phone or in person with banks and credit agencies trying to reverse unauthorized charges, clear up credit issues, and order new cards.

72. The public exposure of the Social Security numbers of tens of thousands of SPE's current and former employees creates serious problems. Neal O'Farrell, a security and identity theft expert for Credit Sesame calls a Social Security number "your secret sauce," that is "as good as your DNA to hackers." Current and former employees have spent time contacting law enforcement and various agencies, such as

the Internal Revenue Service and the Social Security Administration, about the theft of their Social Security numbers. They have already experienced identity theft, identity or medical fraud, and/or now face a real and immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers, and will need to monitor their credit and tax filings for an indefinite duration. Yet, they will have to wait until they become victims of Social Security number misuse before they can obtain a new one. Even then, the Social Security Administration warns "that a new number probably will not solve all [] problems . . . and will not guarantee [] a fresh start." In fact, "[f]or some victims of identity theft, a new number actually creates new problems." One of those new problems is that a new Social Security number will have a completely blank credit history, making it difficult to get credit for a few years unless it is linked to the old compromised number.

73. Current and former SPE employees and family members whose medical and insurance information has been leaked will need to spend time monitoring their financial statements, medical bills, insurance records, utility bills and credit reports for the rest of their lives. They may also be fraudulently charged for unauthorized medical services or equipment, which will require them to spend time and money resolving these problems. They will also have to deal with an increased risk of medical identity theft. Medical information is highly valuable and is reportedly "worth 10 times more than [a person's] credit card number on the black market." The

Office of Inspector General of the U.S. Department of Health & Human Services cautions that "[m]edical identity theft can disrupt your life, damage your credit rating, and waste taxpayer dollars. The damage can be life-threatening to you if the wrong information ends up in your personal medical records."

74. SPE has offered current and former employees twelve months of credit monitoring and identity theft insurance with AllClear ID. But, neither the monitoring nor the insurance can prevent identity theft or fraud, even for the twelve month period. Credit monitoring only informs a consumer of instances of fraudulent opening of new accounts. Identity theft insurance only reimburses losses after they have occurred. Neither of those services prevent identity theft or fraud by: (i) detecting sales of PII on underground black market websites before the PII is used to commit identity theft or identity fraud; (ii) monitoring public records, loan data, or criminal records; (iii) flagging existing accounts for fraud in order to thwart identity thieves' use of compromised PII before an unauthorized transaction can be completed; or (iv) freezing credit, which prevents identity thieves' ability to open new accounts with compromised PII.

75. Sites ranking companies that provide identity protection services have noted that while many of these companies do offer services to prevent identity theft and fraud, AllClear ID's services only assist people that are *already* victims of identity thieves. In fact, these ranking sites regularly give seven or more other

identity services companies a better overall ranking for identity services than AllClear ID.

76. United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected. As Identity Finder LLC CEO Todd Feinman told Law360, the real victims are SPE's current and former employees: "They're now at risk for identity theft for the rest of their lives."

VI. PLAINTIFFS' MOST SENSITIVE INFORMATION IS BREACHED, CAUSING LIFELONG DATA INSECURITY

A. Michael Corona

77. Plaintiff Michael Corona is a former employee of SPE, which employed Plaintiff Corona from 2004 to 2007 in Culver City, California. He is currently a resident of the State of Virginia.

78. In exchange for his employment services, SPE offered to compensate Plaintiff Corona and provide him with other employment benefits. To receive compensation and employment benefits, SPE required Plaintiff Corona to: (i) provide SPE with PII to fulfill SPE's legal responsibilities and operational requirements, including his full name, home address, Social Security Number, as well as PII of people designated as beneficiaries on his employment-related benefits through SPE; (ii) cooperate in providing medical information necessary to determine responsibility for health provider payments; and (iii) provide other confidential information including self-evaluations and, ultimately, his reason for resigning. Plaintiff Corona believes that this was a standard employment agreement that SPE had with its

employees during his tenure at SPE. Plaintiff Corona accepted SPE's employment offer and provided the PII SPE required, expecting that SPE would exercise reasonable care to safeguard and maintain the confidentiality of his PII except to the extent necessary to provide the agreed compensation and other employment benefits. When he ended his employment with SPE, he expected that SPE would destroy or archive his information securely.

79. Plaintiff Corona contacted SPE's human resources department on or about December 2, 2014 after hearing about the Data Breach seeking to learn whether his PII had been compromised. While SPE confirmed receipt of his inquiry, to date, SPE has not substantively responded to his inquiry.

80. Due to SPE's silence, Plaintiff Corona spent 40-50 hours confirming for himself whether the Data Breach compromised his PII, and, on or about December 7, 2014, Plaintiff Corona was able to confirm that his PII was compromised as a result of the Data Breach and that an unencrypted spreadsheet containing his PII had been publicly distributed on the internet, including, but not limited to, his full name, Social Security Number, birthdate, former home address, salary history, and reason for resigning. In addition, due to media reports of medical data and policy numbers being compromised in the Data Breach and his knowledge of SPE correspondence relating to health care provided to him while employed at SPE, Plaintiff Corona believes that his medical information was also compromised by the Data Breach.

81. Upon confirming that his PII was compromised, Plaintiff Corona spent an additional 40-50 hours attempting to contain the impact of the Data Breach on his and his family's identity through the end of December 2014. On or about December 7, 2014, Plaintiff Corona signed up with LifeLock identity protection, monitoring, and recovery services for himself and his family, causing him to incur annual out-of-pocket costs of approximately $700 per year. He then subsequently continued to research ways to contain the impact of SPE's Data Breach on himself and his family members, including: (i) spending hours changing passwords and meticulously combing through emails to delete those containing PII beyond his name and email address; (ii) transferring financial, retirement, utility, and other accounts and/or obtaining new PINs for these accounts; (iii) placing a fraud alert with a credit agency; (iv) learning through his continued research on December 9, 2014 about an SPE email in which SPE former employees could be requested to be added to the AllClear ID program and requesting inclusion in the program; (v) receiving confirmation on December 10, 2014 that SPE had submitted his information to AllClear ID, but needing to contact AllClear ID directly to initiate services; (vi) subsequently contacting AllClear ID to initiate services; (vii) contacting law enforcement authorities pertaining to his compromised PII as a result of the Data Breach; and (viii) filing a complaint with the Federal Trade Commission pertaining to his compromised PII as a result of the Data Breach. If SPE had proactively notified him of the Data Breach and/or responded to his inquiry attempting to confirm that the Data Breach

compromised his PII, he would have attempted to further contain the impact of SPE's Data Breach on his PII by taking these steps sooner.

82. Despite Plaintiff Corona's efforts to contain the impact of SPE's Data Breach on his PII, Plaintiff Corona received further confirmation that his PII had not only been compromised and publicized as a result of the Data Breach, but that an identity thief had used his compromised PII to attempt to open a new bank account. AllClear ID notified him on December 20, 2014 that because Plaintiff Corona had independently acted to place a 90-day fraud alert with a credit agency, the thief's attempt to open the account had been thwarted this time. Nevertheless, Plaintiff Corona understands that he will need to be diligent and renew this fraud alert with a credit agency every 90 days to retain this preventative protection. Going forward, Plaintiff Corona anticipates spending considerable time and money for the rest of his life in order to contain the impact of SPE's Data Breach on himself and his family members, and people designated as beneficiaries on his employment-related benefits through SPE.

B. Christina Mathis

83. Plaintiff Christina Mathis is a former employee of Sony Pictures Consumer Products, a subsidiary of SPE, which employed Plaintiff Mathis from approximately 2000 to 2002 in Culver City, California. She is currently a resident of the State of California. Plaintiff Mathis has not worked for Sony in over 12 years.

84. In exchange for her employment services, SPE offered to compensate Plaintiff Mathis and provide her with other employment benefits. To receive compensation and employment benefits, SPE required Plaintiff Mathis to provide SPE with PII to fulfill SPE's legal responsibilities and operational requirements, including her full name, Social Security Number, home address, as well as PII of beneficiaries of her employment-related benefits through SPE. Plaintiff Mathis accepted SPE's employment offer and provided the PII SPE required, expecting that SPE would exercise reasonable care to safeguard and maintain the confidentiality of her PII except to the extent necessary to provide the agreed compensation and other employment benefits. When she ended her employment with SPE, she expected that SPE would destroy or archive her information securely.

85. Plaintiff Mathis learned about the Data Breach through the Huffington Post on or about December 1, 2014, but believed that the Data Breach compromised only the PII of current SPE employees. On or about December 11, 2014, her further investigation uncovered an email address for former employees that she used to contact SPE seeking to confirm whether her PII had been compromised and to request SPE assistance in containing compromised PII.

86. Despite the fact that she has not worked at SPE for 12 years, on or about December 11, 2014, Plaintiff Mathis was able to confirm through a non-SPE source that her PII was compromised as a result of the Data Breach and that her PII was

publicly available on the internet, including but not limited to her full name, Social Security Number and prior home address.

87. Upon confirming that her PII had been compromised and published to the internet, Plaintiff Mathis spent time enrolling in LifeLock identity protection, monitoring, and recovery services for herself, causing her to incur annual out-of-pocket costs of approximately $300. She subsequently spent many hours continuing to research ways to contain the impact of SPE's Data Breach on her PII, including: (i) contacting her bank to alert them to the compromise of her PII as a result of SPE's Data Breach; (ii) contacting a password protection entity and paying $29.99 to change and manage all of her new passwords; (iii) increasing privacy screens on social media sites; and (iv) placing a 90-day credit fraud alert with a credit service entity. If SPE had proactively notified her of the Data Breach and/or substantively responded to her inquiry attempting to confirm that the Data Breach compromised her PII, she would have attempted to further contain the impact of SPE's Data Breach on her PII by taking these steps sooner.

88. On or about December 18, 2014, Plaintiff Mathis received an email from SPE stating that it was providing AllClear ID's Secure and PRO services for 12 months from the date of the email, which would automatically provide an identity theft investigator if a problem arose, and that she could use a redemption code to sign up for AllClear ID. The email also recommended that Plaintiff Mathis regularly review statements from her accounts and periodically obtain her credit report for

accounts and creditor inquiries that she did not recognize, as well as home addresses and Social Security numbers that were not accurate. It further recommended that she remain vigilant with respect to reviewing her account statements and credit reports and report suspected identity theft to proper law enforcement authorities, including local law enforcement, the state attorney general and/or the Federal Trade Commission. SPE also recommended that she regularly review her explanation of benefits statements from her insurer for unrecognized medical bills. Accordingly, going forward, Plaintiff Mathis anticipates spending considerable time and money for the rest of her life in an effort to contain the impact of SPE's Data Breach on herself and people designated as beneficiaries on her employment-related benefits through SPE.

C. Joshua Forster

89. Plaintiff Joshua Forster is a former employee of Sony Pictures Imageworks, a division of SPE, which employed Plaintiff Forster from approximately January 2013 to April 2013 in California. In addition, Plaintiff Forster worked for SPE as a contractor from approximately April 2013 until February 2014, and worked on and off for various SPE subsidiaries and affiliates from approximately June 2004 to August 2010. He is currently a resident of the State of Colorado.

90. In exchange for his employment services, SPE offered to compensate Plaintiff Forster and provide him with other employment benefits. To receive compensation and employment benefits, SPE required Plaintiff Forster to: (i) provide

SPE with PII to fulfill SPE's legal responsibilities and operational requirements, including his: full name, home address, telephone number, date of birth, Social Security Number, direct deposit routing instructions, copies of his driver's license, Social Security card, and resident alien card, as well as PII of beneficiaries of his employment-related benefits through SPE; (ii) cooperate in providing information about his health condition to receive medical care from SPE's on-site medical facility; and (iii) provide other confidential information including his credit card information in order to make purchases from SPE's on-site store and information necessary for SPE to run a background check. Plaintiff Forster accepted SPE's employment offer and provided the PII SPE required, expecting that SPE would exercise reasonable care to safeguard and maintain the confidentiality of his PII except to the extent necessary to provide the agreed compensation and other employment benefits. When he ended his employment with SPE, he expected that SPE would destroy or archive his information securely.

91. Plaintiff Forster learned of SPE's Data Breach from speaking with relatives who were employed by SPE at the time of the Data Breach on or about November 24, 2014, and later watching the news on television that reported on the Data Breach. Plaintiff Forster subsequently spent approximately 15 hours further investigating the Data Breach and obtained SPE files that were publicly available on the internet, on or about December 6, 2014, from which he confirmed that the Data Breach had compromised his PII, including his name, home address, Social Security

Number, date of birth, telephone number, SPE title, salary, the management structure of his SPE group, and information regarding the insurance carrier, plan, and premiums paid for his medical insurance coverage provided through SPE as a dependent of another SPE employee.

92. Plaintiff Forster's further investigation uncovered information, on or about December 8, 2014, of an email address that he used to contact SPE seeking SPE's assistance in containing compromised PII. SPE informed Plaintiff Forster, on or about December 9, 2014, that AllClear ID would contact him with further information, which was ultimately provided by email on December 12, 2014 along with a redemption code for 12 months of AllClear ID credit monitoring at SPE's expense. Plaintiff Forster also spent time cancelling credit cards, obtaining new credit cards and resetting automatic billing instructions, as well as contacting a credit bureau to set up fraud alerts during this timeframe. If SPE had notified him earlier about the Data Breach and provided him information on how to contain the potential compromise of his PII, Plaintiff Forster would have been able to take these steps to contain the compromise of his PII more quickly.

93. Despite Plaintiff Forster's efforts to contain the compromise of his PII, he learned in or about January 2015 that someone was using his PII to attempt to open a PayPal credit card under his name. While Plaintiff Forster had previously used the AllClear ID redemption code to obtain credit monitoring, he did not learn of the unauthorized use of his PII from AllClear ID, but from PayPal. Plaintiff Forster

then contacted AllClear ID to let it know of this unauthorized use of his PII, which informed him that because one of the credit bureau agencies did not have his date of birth on file, AllClear ID could not confirm his identity and therefore had not initiated his subscription. Prior to Plaintiff Forster contacting AllClear ID, AllClear ID had not attempted to contact him about his registration issues. Plaintiff Forster ultimately received confirmation of his registration for AllClear ID credit monitoring on or about January 20, 2015, about a month after he had used his redemption code to sign up for AllClear ID credit monitoring.

94. Plaintiff Forster continued his efforts to contain the compromise of his PII in late January 2015 by changing his bank account information, which required multiple personal visits to his bank because his account was linked to a relative's account who lives over a thousand miles away and both Plaintiff Forster and his relative needed to be personally present for the bank to change this information. Going forward, Plaintiff Forster anticipates spending considerable time and money for the rest of his life in order to contain the impact of SPE's Data Breach on himself, his relative that was linked to his bank account, and people designated as beneficiaries on his employment-related benefits through SPE.

D. Ella Carline Archibeque

95. Plaintiff Ella Carline Archibeque is a former employee of Sony Pictures Imageworks, a division of SPE, which employed Plaintiff Archibeque at various

times from approximately April 2002 through May 2009 in Culver City, California. She is currently a resident of the State of California.

96. In exchange for her employment services, SPE offered to compensate Plaintiff Archibeque and provide her with other employment benefits. To receive compensation and employment benefits, SPE required Plaintiff Archibeque to provide SPE with PII to: (i) fulfill SPE's legal responsibilities and operational requirements, including her name, home address, email address, Social Security Number, date of birth, copy of her passport and driver's license, IRS W-4 Employee Withholding Allowance Certification information (including marital status), and bank routing information, as well as PII of designated beneficiaries on her employment-related benefits plans offered through SPE, (ii) obtain medical insurance offered by SPE as an employment benefit; and (iii) other confidential information including information needed for SPE to obtain a background check. Plaintiff Archibeque accepted SPE's employment offer and provided the PII SPE required, expecting that SPE would exercise reasonable care to safeguard and maintain the confidentiality of her PII except to the extent necessary to provide the agreed compensation and other employment benefits. When she ended her employment with SPE, she expected that SPE would destroy or archive her information securely.

97. Plaintiff Archibeque first heard about the Data Breach in late November 2014. As the media continued to report on the increasing scope of the Data Breach in early December, SPE remained silent about its extent. Plaintiff Archibeque acted to

contain the potential impact of the Data Breach on her PII. For example, she enrolled in LifeLock identity protection, monitoring, and recovery services for herself, in or about early December, causing her to incur annual out-of-pocket costs of approximately $240 per year. As she continued to investigate published information about the Data Breach, she obtained an email address designated for former employees to contact SPE about the Data Breach. She then contacted SPE by email, on or about December 9, 2014, at this address, seeking to confirm whether the Data Breach had compromised her PII. SPE responded to her email, on or about December 10, 2014, with an AllClear ID offer.

98. Despite Plaintiff Archibeque's efforts to contain the impact of SPE's Data Breach on her PII, Plaintiff Archibeque received confirmation that her PII had not only been compromised and publicized as a result of the Data Breach, but that her PII was being sold on the black market. On December 10, 2014, LifeLock provided Plaintiff Archibeque with a Black Market Website Notification which stated that LifeLock had detected that her email address and password was being sold on a black market website. In response to this notification, she has frozen her credit, and placed a fraud alert with the Internal Revenue Service and a credit agency. If SPE had proactively notified Plaintiff Archibeque about the Data Breach, she would have attempted to further contain the impact of SPE's Data Breach on her PII by taking these steps sooner. Going forward, Plaintiff Archibeque anticipates spending considerable time and money for the rest of her life in an effort to contain the impact

of SPE's Data Breach on herself and people designated as beneficiaries on her employment-related benefits through SPE.

E. Michael Levine

99. Plaintiff Michael Levine is a former employee of Sony Pictures Imageworks, a division of SPE, which employed Plaintiff Levine from approximately 2003 to 2012 in California. He is currently a resident of California.

100. In exchange for his employment services and consent to use his image for promotional purposes, SPE offered to compensate Plaintiff Levine and provide him with other employment benefits. To receive compensation and employment benefits, SPE required Plaintiff Levine to: (i) provide SPE with PII to fulfill SPE's legal responsibilities and operational requirements, including his: full name, home address, date of birth, Social Security Number, and direct deposit routing instructions, as well as PII of people designated as beneficiaries on his employment-related benefits through SPE; (ii) cooperate in providing medical information relevant to health insurance coverage; and (iii) provide other confidential information including his employment and educational history. Plaintiff Levine accepted SPE's employment offer and provided the PII SPE required, expecting that SPE would exercise reasonable care to safeguard and maintain the confidentiality of his PII except to the extent necessary to provide the agreed compensation and other employment benefits. When he ended his employment with SPE, he expected that SPE would destroy or archive his information securely.

101. Plaintiff Levine learned of SPE's Data Breach, on or about the end of November 2014, through an article written in *Variety*. Plaintiff Levine subsequently spent approximately 40 hours further investigating the Data Breach during the next approximately two weeks and ultimately obtained the SPE master index file that was publicly available on the internet, from which he confirmed that the Data Breach had compromised his PII, including his name, employment offer letters, and payroll information, including his Social Security Number.

102. Within approximately a week of confirming that his PII had been compromised in the Data Breach, Plaintiff Levine continued investigating ways to contain the impact of the Data Breach on himself and family. He contacted SPE by sending three separate emails seeking guidance in relation to this issue, but received only a single generic response from SPE several weeks later offering 12 months of AllClear ID identity theft investigation and credit monitoring services at its expense to current and former employees with potentially compromised PII as a result of the Data Breach.

103. While he was awaiting a response from SPE to his inquiries, Plaintiff Levine spent 30 to 40 hours continuing to investigate how to contain the impact of the SPE Data Breach on himself and his family, and acted to contain this impact by: (i) freezing his credit so that new credit card accounts could not be opened and new bank loans could not be obtained with his compromised PII, resulting in $50 in out-of-pocket costs to date; (ii) upgrading his family's AAA membership to AAA Plus in

order to obtain monthly credit monitoring and credit fraud notification services, at an added annual expense of $50; (iii) notifying the Internal Revenue Service that his Social Security Number had been compromised as a result of the Data Breach; and (iv) placing fraud alerts with Experian, Equifax, TransUnion, and his other financial accounts.

104. If SPE had proactively notified him of the Data Breach and promptly responded to his inquiries for more information, Plaintiff Levine would have been able to take these steps more quickly because he would not have had to spend so much time researching how to contain the impact of the Data Breach on himself and his family. Going forward, Plaintiff Levine anticipates spending considerable time and money for the rest of his life in an effort to contain the impact of SPE's Data Breach on himself, his family, and people designated as beneficiaries on his employment-related benefits through SPE.

F. Geoffrey Springer

105. Plaintiff Geoffrey Springer is a former employee of SPE, which employed Springer from approximately October 1995 to August 1997 and again from approximately April 2000 through December 2004 in California. He is currently a resident of the State of Virginia.

106. In exchange for his employment services and his agreement not to compete with SPE for a certain time period after leaving employment with SPE, SPE offered to compensate Plaintiff Springer and provide him with other employment

benefits. To receive compensation and employment benefits, SPE required Plaintiff Springer to: (i) provide SPE with PII to fulfill SPE's legal responsibilities and operational requirements, including his full name, home address, Social Security Number, date of birth, bank account electronic deposit information, as well as PII of people designated as beneficiaries on his employment-related benefits through SPE; (ii) cooperate in providing medical information necessary to treat him in the event of a workplace medical emergency, including his health care providers and preferred hospital; and (iii) provide other confidential information including employment and education history. Plaintiff Springer accepted SPE's employment offer and provided the PII SPE required, expecting that SPE would exercise reasonable care to safeguard and maintain the confidentiality of his PII except to the extent necessary to provide the agreed compensation and other employment benefits. When he ended his employment with SPE, he expected that SPE would destroy or archive his information securely.

107. Plaintiff Springer initially heard of SPE's Data Breach around Thanksgiving 2014, when he was watching news that included a report on the Data Breach. On or about the first week of December 2014, Plaintiff Springer obtained an unencrypted publicly available SPE file from the internet and confirmed that this file contained his PII, including his name, Social Security Number, home address during his employment at SPE, job title and date of separation from SPE.

108. After Plaintiff Springer confirmed that the Data Breach had compromised his PII, he reached out to SPE's human resources department and learned that SPE had created an email address box for former employees to contact in order to obtain one year of credit monitoring through AllClear ID at SPE's expense.

109. Plaintiff Springer then spent approximately 15 hours evaluating AllClear ID and other competing identity protection services, and concluded that paying to protect his PII through LifeLock would minimize his losses if his PII was to be used by an identity thief because it not only monitored credit reporting agencies, but also credit card purchasing information, bank account transactions, and scanned the dark web. On or about mid-December, Plaintiff Springer paid to obtain these services from LifeLock for himself, causing him to incur annual out-of-pocket costs of more than $350 per year.

110. Plaintiff Springer subsequently spent approximately 40 hours continuing to research ways to contain the impact of SPE's Data Breach, including: placing a security freeze on his credit, making advance arrangements for a timeframe to unlock and re-freeze his credit so that he could purchase a vehicle, and paying $30, so far, to freeze, unfreeze, and re-freeze his credit, placing fraud alerts with credit reporting agencies Experian, Equifax, and TransUnion, contacting the Internal Revenue Service and informing them that his Social Security Number had been compromised in the Data Breach, and resetting his car and mortgage automatic payment instructions. If SPE had notified him earlier about the Data Breach and provided him information on

how to contain the potential compromise of his PII, Plaintiff Springer would have been able to take these steps to contain the compromise of his PII more quickly. Going forward, Plaintiff Springer anticipates spending considerable time and money for the rest of his life in order to contain the impact of SPE's Data Breach on himself and people designated as beneficiaries on his employment-related benefits through SPE.

G. Marcela Bailey

111. Plaintiff Marcela Bailey is a former employee of SPE, which employed Plaintiff Bailey from approximately January 1991 to February 2013. She is currently a resident of California.

112. In exchange for her employment services, SPE offered to compensate Plaintiff Bailey and provide her with other employment benefits. To receive compensation and employment benefits, SPE required Plaintiff Bailey to provide SPE with PII to fulfill SPE's legal responsibilities and operational requirements, including (i): her name, home address, telephone number, Social Security Number, date of birth, marital status, signature, physical characteristics description, passport number, copy of her Visa, driver's license number, direct deposit routing instructions, as well as PII of her dependents and people designated as beneficiaries on her employment-related benefits through SPE; (ii) medical and health insurance information; and (iii) other confidential information including education and employment history, financial information including credit card numbers and investment information, personnel file

information, passwords, and educational information for tuition reimbursement. Plaintiff Bailey accepted SPE's employment offer and provided the PII SPE required, expecting that SPE would exercise reasonable care to safeguard and maintain the confidentiality of her PII and other confidential information except to the extent necessary to provide the agreed compensation and other employment benefits. When she ended her employment with SPE, she expected that SPE would destroy or archive her information securely.

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

danger of being disclosed. Throughout the evening, Plaintiff Bailey also had heard various breaking news reports regarding the security breach at SPE.

114. Due to SPE's failure to substantively respond to her inquiries and update her with information, Plaintiff Bailey expended 30 to 40 hours and incurred expenses attempting to protect her and her family's PII from unauthorized use, including: purchasing LifeLock's identity theft protection services for her family on or about December 15, 2014, for which she has incurred out-of-pocket expenses of over $1000 and will incur out-of-pocket expenses of more than $1000 annually, monitoring and changing bank and credit accounts, placing credit freezes, and closely monitoring news coverage and reports pertaining to the breach.

115. Despite her efforts to contain the impact of the Data Breach on the PII of her family and herself, Plaintiff Bailey received confirmation that her PII was being sold on the black market. On or about December 17, 2014, Plaintiff Bailey received a black market alert from LifeLock that notified her that her name and Social Security Number were being sold on an illegal black market website.

116. Plaintiff Bailey received further confirmation that her family's PII had not only been compromised in the Data Breach, but was also being used by an identity thief. Specifically, an identity thief appears to have succeeded in making unauthorized cash withdrawals on her husband's bank account, causing her family to incur overdraft charges and spending 10 hours making a claim and replacing the affected debit card.

117. Going forward, Plaintiff Bailey anticipates spending considerable time and money for the rest of her life in an effort to contain the impact of SPE's Data Breach on herself, her family, and people designated as beneficiaries on her employment-related benefits through SPE.

H. Steven Shapiro

118. Plaintiff Steven Shapiro is a former employee of Sony Pictures Imageworks, a division of SPE, which employed Plaintiff Shapiro from approximately October 2003 through January 2010 in California. He is currently a resident of California.

119. In exchange for his employment services, SPE offered to compensate Plaintiff Shapiro and provide him with other employment benefits. To receive compensation and employment benefits, SPE required Plaintiff Shapiro to provide SPE with PII to fulfill SPE's legal responsibilities and operational requirements, including: (i) his full name, home address, Social Security Number, copy of his driver's license and passport, bank wiring instructions for direct deposits, as well as PII of people designated as beneficiaries on his employment-related benefits through SPE; and (ii) medical information about major procedures and medical insurance claims. Plaintiff Shapiro accepted SPE's employment offer and provided the PII SPE required, expecting that SPE would exercise reasonable care to safeguard and maintain the confidentiality of his PII except to the extent necessary to provide the agreed compensation and other employment benefits. When he ended his

employment with SPE, he expected that SPE would destroy or archive his information securely.

120. Plaintiff Shapiro first learned of the Data Breach from an online media site that SPE employee data was compromised by the Data Breach on or about November 27, 2014.

121. Plaintiff Shapiro thus contacted SPE on or about December 5, 2014 seeking to confirm whether his PII had been compromised as a result of the Data Breach and sought to learn how to contain the potential damage to his identity. SPE acknowledged Plaintiff Shapiro's inquiry on December 8, 2014, and told him that it may take several days for SPE to substantively respond. On December 11, 2014, SPE informed him that it was working to provide 12 months of AllClear ID credit monitoring services, at SPE's expense, to potentially impacted employees and former employees (and their dependents), but, would not be offering these services to named beneficiaries who are not dependents of employees or former employees. To date, SPE has not confirmed whether or not Plaintiff Shapiro's PII was in fact compromised through the Data Breach.

122. Due to SPE's delay and failure to date to substantively respond to his inquiry, Plaintiff Shapiro has spent between 100 and 150 hours confirming whether the Data Breach compromised his PII over several weeks. He ultimately obtained SPE files that were publicly available on the internet that confirmed that his PII, including his name, address, Social Security Number, salary, reason for leaving SPE,

position, and checking account information, was compromised and released as a result of the Data Breach in or about mid-December 2014. Plaintiff Shapiro also confirmed that this information was available for anyone to download, including anyone who would want to sell it on the black market. Plaintiff Shapiro also believes that his medical information may have been compromised because he heard that medical information regarding major medical procedures performed on SPE employees was also compromised in the Data Breach.

123. Plaintiff Shapiro subsequently spent significant time attempting to contain the impact of the compromised PII on his identity by: (i) spending approximately four hours placing a credit freeze with four credit bureaus, requiring him to pay $40; (ii) spending approximately 30 hours managing the aftermath of his credit being frozen, including difficulty setting up new utilities after moving and problems obtaining a lease for a new home, which has required him to pay $30 to unfreeze his credit; (iii) paying $50 to obtain all of his credit reports and credit scores which were required by his new landlord because of difficulties that his landlord had in reviewing his credit; and (iv) changing his bank account, which required spending time tracking outstanding checks from his old accounts that needed to be cashed before he could close it, as well as depositing a minimum deposit in his new account to avoid re-issued checking fees and updating all of his utilities and other vendors that were automatically billed and being paid from his prior bank account.

124. Going forward, Plaintiff Shapiro anticipates spending considerable time and money for the rest of his life in an effort to contain the impact of SPE's Data Breach on himself and people designated as beneficiaries on his employment-related benefits through SPE.

I. Lawon Exum

125. Plaintiff Lawon Exum is a former employee of SPE, which employed Plaintiff Exum from approximately 2005 to 2014 in Culver City, California. He is currently a resident of the State of California.

126. In exchange for his employment services, SPE offered to compensate Plaintiff Exum and provide him with other employment benefits. To receive compensation and employment benefits, SPE required Plaintiff Exum to provide SPE with PII to fulfill SPE's legal responsibilities and operational requirements, including his full name, Social Security Number and home address, as well as PII of people designated as beneficiaries on his employment-related benefits through SPE. Plaintiff Exum accepted SPE's employment offer and provided the PII SPE required, expecting that SPE would exercise reasonable care to safeguard and maintain the confidentiality of his PII except to the extent necessary to provide the agreed-upon compensation and other employment benefits. When he ended his employment with SPE, he expected that SPE would destroy or archive his information securely.

127. Plaintiff Exum learned about the Data Breach on or about November 24, 2014, and immediately sent an email to SPE to confirm whether his PII had been compromised and to request SPE's assistance in containing his compromised PII.

128. Plaintiff Exum was able to confirm on or about December 12, 2014 through investigation and filing his yearly income tax return, that his PII was compromised in the Data Breach and that the hackers publicly distributed his PII on the internet, including but not limited to his full name, Social Security number and home address.

129. Upon confirming that his PII had been compromised, Plaintiff Exum spent approximately 80 hours contacting his creditors, financial institutions, and the three credit bureaus. A block was placed on his credit reports which led to a denial of credit. He was unable to open a checking account or receive further credit from his credit union due to the blocks placed on his credit reports. He incurred late/declined payment fees as a result of failed automatic payments. Additionally, he contacted the Culver City Police Department and the Internal Revenue Service to make them aware of the situation and to inquire about his PII being compromised. Plaintiff Exum incurred out-of-pocket costs of approximately $500 in these efforts. If SPE had proactively notified him of the Data Breach or responded to his inquiry, he would have been able to take these steps sooner.

130. On or about December 28, 2014, Plaintiff Exum received a letter from SPE written to provide employees information about the Data Breach. The letter was

dated December 17, 2014, but Plaintiff Exum did not receive it until December 28, 2014. Going forward, Plaintiff Exum anticipates spending considerable time and money for the rest of his life in an effort to contain the impact of SPE's Data Breach on himself and people designated as beneficiaries on his employment-related benefits through SPE.

VII. CLASS ACTION ALLEGATIONS

131. Plaintiffs bring claims pursuant to Federal Rule of Civil Procedure 23 on behalf of classes of similarly situated persons, which they initially propose be defined as follows:

Nationwide Class

All current and former SPE employees in the United States whose PII was compromised as a result of the data breach publicized in November 2014.

California Class

All current and former SPE employees who reside or have resided in California and whose PII was compromised as a result of the data breach publicized in November 2014.

Virginia Class

All current and former SPE employees who reside or have resided in Virginia and whose PII was compromised as a result of the data breach publicized in November 2014.

Colorado Class

All current and former SPE employees who reside or have resided in Colorado and whose PII was compromised as a result of the data breach publicized in November 2014.

132. **Numerosity.** The proposed classes are sufficiently numerous, as thousands of current and former SPE employees have had their PII compromised. The class members are so numerous and dispersed throughout the United States that joinder of all members is impracticable. Class members can be readily identified by records maintained by SPE.

133. **Commonality.** Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual class members.

For the Nationwide Class, common questions include:

a. Whether SPE had a legal duty to use reasonable security measures to protect class members' PII;

b. Whether SPE timely, accurately, and adequately informed class members that their PII had been compromised;

c. Whether SPE breached its legal duty by failing to protect class members' PII;

d. Whether SPE acted reasonably in securing class members' PII;

e. Whether class members are entitled to actual damages and/or statutory damages; and

f. Whether class members are entitled to injunctive relief.

For the California Class, common questions include:

a. Whether SPE violated Civil Code section 1798.81.5 by failing to implement reasonable security procedures and practices;

b. Whether SPE violated Civil Code section 1798.82 by failing to promptly notify class members that their personal information had been compromised;

c. Whether the information stolen in the Data Breach was "personal information" as defined by Civil Code sections 1798.80(e) and 1798.81.5(d);

d. Whether class members are entitled to damages; and

e. Whether class members are entitled to injunctive relief.

For the Virginia Class, common questions include:

a. Whether SPE violated Virginia Code Annotated section 18.2-186.6(B) by failing to promptly notify class members that their personal information had been compromised;

b. Whether the information compromised by the Data Breach was "personal information" as defined by section 18.2-186.6(A);

c. Whether class members are entitled to damages; and

d. Whether class members are entitled to injunctive relief.

For the Colorado Class, common questions include:

a. Whether SPE violated Colorado Revised Statutes Annotated section 6-1-716(2) by failing to promptly notify class members that their personal information had been compromised;

b. Whether the information compromised by the Data Breach constituted "personal information" as defined by section 6-1-716(1)(d);

c. Whether class members are entitled to damages; and

d. Whether class members are entitled to injunctive relief.

134. **Typicality.** Plaintiffs' claims are typical of the claims of members of the proposed classes because, among other things, Plaintiffs and class members sustained similar injuries as a result of SPE's uniform wrongful conduct and their legal claims all arise from the same conduct by SPE.

135. **Adequacy.** Plaintiffs will fairly and adequately protect the interests of the proposed classes. Their interests do not conflict with class members' interests and they have retained counsel experienced in complex class action and data privacy litigation to prosecute this case on behalf of the classes.

136. **Rule 23(b)(3).** In addition to satisfying the prerequisites of Rule 23(a), Plaintiffs satisfy the requirements for maintaining a class action under Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual class members and a class action is superior to individual litigation. The amount of damages available to individual plaintiffs is insufficient to make litigation addressing SPE's conduct economically feasible in the absence of the class action procedure. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the

court system presented by the legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

137. **Rule 23(b)(2).** Plaintiffs also satisfy the requirements for maintaining a class action under Rule 23(b)(2). SPE has acted or refused to act on grounds that apply generally to the proposed classes, making final declaratory or injunctive relief appropriate with respect to the proposed classes as a whole.

138. **Rule 23(c)(4).** Plaintiffs also satisfy the requirements for maintaining a class action under Rule 23(c)(4). The claims of class members are composed of particular issues that are common to all class members and capable of class wide resolution that will significantly advance the litigation.

VIII. CAUSES OF ACTION

COUNT I: Negligence

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

140. Plaintiffs bring this cause of action on behalf of the Nationwide Class.

141. In collecting the financial, medical and other personal information of its employees, SPE as an employer owed Plaintiffs and class members a duty to exercise reasonable care in safeguarding and protecting that information. This duty included, among other things, maintaining and testing SPE's security systems and taking other

reasonable security measures to protect and adequately secure the PII of Plaintiffs and class members from unauthorized access.

142. SPE's security system and procedures for handling the financial, medical and other personal information of its current and former employees were intended to and did affect Plaintiffs and class members. SPE knew that by collecting and storing its employees' sensitive personal, financial and medical information, it undertook a responsibility to take reasonable security measures to protect the information from being stolen and exposed to unauthorized persons.

143. SPE owed a duty of care to Plaintiffs and class members because they were foreseeable and probable victims of any inadequate security practices. It was foreseeable that if SPE did not take reasonable security measures, the PII of Plaintiffs and members of the class would be stolen. Major corporations like SPE face a higher threat of security breaches than smaller companies due in part to the large amounts of data they possess. SPE knew or should have known its security systems were inadequate, particularly in light of the prior data breaches that SPE and its sister companies have experienced, and yet SPE failed to take reasonable precautions to safeguard the PII of its current and former employees.

144. The duty SPE owed to Plaintiffs and members of the class to protect their PII is also underscored by the California Customer Records Act, the Confidentiality of Medical Information Act and Health Insurance Portability and Accountability Act ("HIPAA"), which recognize the importance of maintaining the

confidentiality of personal and medical information and were enacted to protect individuals from the unauthorized exposure of their personal and medical information.

145. SPE also had a duty to timely disclose to Plaintiffs and class members that their personal information had been or was reasonably believed to have been compromised. Timely disclosure was necessary so that Plaintiffs and members of the class could, among other things: (i) buy identity protection, monitoring, and recovery services; (ii) flag asset, credit, and tax accounts for fraud, including reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the Internal Revenue Service; (iii) purchase or otherwise obtain credit reports; (iv) monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit inquiries, Social Security numbers, home addresses, charges, and/or medical services; (v) place and renew credit fraud alerts on a quarterly basis; (vi) routinely monitor public records, loan data, or criminal records; (vii) contest fraudulent charges and other forms of criminal, financial and medical identity theft, and repair damage to credit and other financial accounts; and (viii) take other steps to protect themselves and recover from identity theft and fraud.

146. SPE has admitted that its current and former employees' PII was exposed as a result of the Data Breach. As a result of SPE's negligence, Plaintiffs and members of the class have suffered and will suffer injury, including but not necessarily limited to: (1) the loss of the opportunity to control how their PII is used;

(2) the diminution in the value and/or use of their PII entrusted to SPE for the purpose of deriving employment from SPE and with the understanding that SPE would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, publication, and/or theft of their PII and the PII of their family members and designated beneficiaries of employment-related benefits through SPE; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity and health care/medical data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets; (7) unauthorized use of compromised PII to open new financial and/or health care or medical accounts; (8) tax fraud and/or other unauthorized charges to financial, health care or medical accounts and associated lack of access to funds while proper information is confirmed and corrected; (9) the continued risk to their PII, and the PII of their family members and designated beneficiaries of employment-related benefits through SPE, which remain in SPE's possession and are subject to further breaches so long as SPE fails to undertake appropriate and adequate measures to protect the PII in its possession; and (10) future

costs in terms of time, effort and money that will be expended, to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of the Nationwide Class members, their families, and their designated beneficiaries of employment-related benefits through SPE.

147. There is a very close connection between SPE's failure to employ reasonable security protections of its current and former employees' PII and the injuries suffered by Plaintiffs and class members. When individuals have their PII stolen, they are at risk for identity theft, and need to: (i) buy identity protection, monitoring, and recovery services; (ii) flag asset, credit, and tax accounts for fraud, including reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the Internal Revenue Service; (iii) purchase or otherwise obtain credit reports; (iv) monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit inquiries, Social Security numbers, home addresses, charges, and/or medical services; (v) place and renew credit fraud alerts on a quarterly basis; (vi) routinely monitor public records, loan data, or criminal records; (vii) contest fraudulent charges and other forms of criminal, financial and medical identity theft, and repair damage to credit and other financial accounts; and (viii) take other steps to protect themselves and recover from identity theft and fraud.

148. SPE is responsible for not protecting the PII of its current and former employees. If SPE had reasonable security measures in place, data thieves would not

have been able to steal and expose the PII of thousands of current and former SPE employees.

149. The policy of preventing future harm weighs strongly in favor of finding a special relationship between SPE and its current and former employees. SPE's employees were required to share sensitive personal and medical information with SPE as a condition of employment and depended on SPE as their employer to ensure that this information is protected from theft and unauthorized disclosure. If companies are not held accountable for failing to take reasonable security measures to protect their employees' PII, they will not take the steps that are necessary to protect against future data breaches.

150. SPE breached its duty to exercise reasonable care in protecting the PII of Plaintiffs and the class by failing to implement and maintain adequate security measures to safeguard its employees' PII, failing to monitor its systems to identify suspicious activity, and allowing unauthorized access to the PII of Plaintiffs and class members.

151. SPE breached its duty to timely notify Plaintiffs and the class about the Data Breach. SPE waited several days after discovering the Data Breach to inform its current employees that their PII had been or was reasonably believed to have been compromised, and waited even longer to issue a notice to its former employees affected by the breach. SPE has yet to notify some former employees.

152. But for SPE's failure to implement and maintain adequate security measures to protect its employees' PII and failure to monitor its systems to identify suspicious activity, the PII of Plaintiffs and class members would not have been stolen, Plaintiffs and class members would not have been injured, and Plaintiffs and class members would not be at a heightened risk of identity theft in the future.

153. SPE's negligence was a substantial factor in causing harm to Plaintiffs and class members. As a direct and proximate result of SPE's failure to exercise reasonable care and use commercially reasonable security measures, the PII of SPE's current and former employees was accessed by unauthorized individuals who: (i) have already used the compromised information to commit identity theft and fraud; (ii) can continue to use this compromised PII to commit identity theft and identity and health care and/or medical fraud; and (iii) have posted the information on the internet, allowing themselves and others to commit identity theft, and identity and health care and/or medical fraud using the compromised PII indefinitely.

154. As a result of SPE's negligence, Plaintiffs and members of the class are entitled to injunctive relief, including, but not limited to an order that SPE: (1) engage third party security auditors/penetration testers as well as internal security personnel to conduct testing consistent with prudent industry practices, including simulated attacks, penetration tests, and audits on SPE's systems on a periodic basis; (2) engage third party security auditors and internal personnel to run automated security monitoring consistent with prudent industry practices; (3) audit, test, and train its

security personnel regarding any new or modified procedures; (4) purge, delete and destroy, in a secure manner, employee data not necessary for its business operations; (5) conduct regular database scanning and securing checks consistent with prudent industry practices; (6) periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach consistent with prudent industry practices; (7) receive periodic compliance audits by a third party regarding the security of the computer systems SPE uses to store the personal information of its current and former employees; (8) meaningfully educate its current and former employees about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves; and (9) provide ongoing identity theft protection, monitoring, and recovery services to Plaintiffs and class members, as well as their dependents and designated beneficiaries of employment-related benefits through SPE.

155. Plaintiffs and the class are also entitled to damages and reasonable attorneys' fees and costs. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

COUNT II: Breach of Implied Contract

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

157. Plaintiffs bring this cause of action on behalf of the Nationwide Class.

158. SPE offered employment to Plaintiffs and class members in exchange for compensation and other employment benefits. To receive compensation and other employment benefits, SPE required Plaintiffs and class members to provide their PII, including names, addresses, Social Security numbers, medical information, and other personal information.

159. SPE had an implied duty of good faith to ensure that the PII of Plaintiffs and class members in its possession was only used to provide the agreed-upon compensation and other employment benefits from SPE.

160. SPE was therefore required to reasonably safeguard and protect the PII of Plaintiffs and class members from unauthorized uses, and to timely and accurately notify Plaintiffs and class members if their PII was compromised so that Plaintiffs and class members could act to mitigate the harm caused by the loss of opportunity to control how their PII was used.

161. Plaintiffs and class members accepted SPE's employment offer and fully performed their obligations under the implied contract with SPE by providing their PII to SPE, among other obligations.

162. Plaintiffs and class members would not have provided and entrusted their PII to SPE in the absence of their implied contracts with SPE, and would have instead retained the opportunity to control their PII for uses other than compensation and other employment benefits from SPE.

163. SPE breached the implied contracts with Plaintiffs and class members by failing to reasonably safeguard and protect Plaintiffs' and class members' PII and by failing to provide timely and accurate notice to Plaintiffs and class members that their PII was compromised as a result of the Data Breach.

164. As a proximate and direct result of SPE's breaches of its implied contracts with Plaintiffs and class members, Plaintiffs and class members have suffered and will suffer injury, including but not necessarily limited to: (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to SPE for the purpose of deriving employment from SPE and with the understanding that SPE would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, publication, and/or theft of their PII and the PII of their family members and designated beneficiaries of employment-related benefits through SPE; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts; (5) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity and health care/medical data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports

and assets; (7) unauthorized use of compromised PII to open new financial and/or health care or medical accounts; (8) tax fraud and/or other unauthorized charges to financial, health care or medical accounts and associated lack of access to funds while proper information is confirmed and corrected; (9) the continued risk to their PII, and the PII of their family members and designated beneficiaries of employment-related benefits through SPE, which remain in SPE's possession and are subject to further breaches so long as SPE fails to undertake appropriate and adequate measures to protect the PII in its possession; and (10) future costs in terms of time, effort and money that will be expended, to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of the Nationwide Class members, their families, and their designated beneficiaries of employment-related benefits through SPE.

COUNT III: Violation of the California Customer Records Act
California Civil Code Section 1798.80 *et seq*.

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

166. Plaintiffs bring this cause of action on behalf of the California Class.

167. The California Legislature enacted Civil Code section 1798.81.5 "to ensure that personal information about California residents is protected." The statute requires that any business that "owns, licenses, or maintains personal information about a California resident … implement and maintain reasonable security procedures

and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

168. SPE is a "business" as defined by Civil Code section 1798.80(a).

169. Each Plaintiff and member of the class is an "individual" as defined by Civil Code section 1798.80(d).

170. The employee information taken in the Data Breach was "personal information" as defined by Civil Code sections 1798.80(e) and 1798.81.5(d), which includes "information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, Social Security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information."

171. The breach of the personal information of thousands of current and former SPE employees was a "breach of the security system" of SPE as defined by Civil Code section 1798.82(g).

172. By failing to implement reasonable security measures appropriate to the nature of the personal information of its current and former employees, SPE violated Civil Code section 1798.81.5.

173. In addition, by failing to immediately notify all affected current and former SPE employees that their personal information had been acquired (or was reasonably believed to have been acquired) by unauthorized persons in the Data Breach, SPE violated Civil Code section 1798.82 of the same title. SPE's failure to immediately notify employees of the breach caused class members to suffer damages because they have lost the opportunity to immediately: (i) buy identity protection, monitoring, and recovery services; (ii) flag asset, credit, and tax accounts for fraud, including reporting the theft of their Social Security numbers to financial institutions, credit agencies, and the Internal Revenue Service; (iii) purchase or otherwise obtain credit reports; (iv) monitor credit, financial, utility, explanation of benefits, and other account statements on a monthly basis for unrecognized credit inquiries, Social Security numbers, home addresses, charges, and/or medical services; (v) place and renew credit fraud alerts on a quarterly basis; (vi) routinely monitor public records, loan data, or criminal records; (vii) contest fraudulent charges and other forms of criminal, financial and medical identity theft, and repair damage to credit and other financial accounts; and (viii) take other steps to protect themselves and recover from identity theft and fraud.

174. Because it violated Civil Code sections 1798.81.5 and 1798.82, SPE "may be enjoined" under Civil Code section 1798.84(e).

175. Plaintiffs request that the Court enter an injunction requiring SPE to implement and maintain reasonable security procedures to protect its employees' PII,

including, but not limited to, ordering that SPE: (1) engage third party security auditors/penetration testers as well as internal security personnel to conduct testing consistent with prudent industry practices, including simulated attacks, penetration tests, and audits on SPE's systems on a periodic basis; (2) engage third party security auditors and internal personnel to run automated security monitoring consistent with prudent industry practices; (3) audit, test, and train its security personnel regarding any new or modified procedures; (4) purge, delete and destroy, in a secure manner, employee data not necessary for its business operations; (5) conduct regular database scanning and securing checks consistent with prudent industry practices; (6) periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach consistent with prudent industry practices; (7) receive periodic compliance audits by a third party regarding the security of the computer systems SPE uses to store the personal information of its current and former employees; (8) meaningfully educate its current and former employees about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves; and (9) provide ongoing identity theft protection, monitoring, and recovery services to Plaintiffs and class members, as well as their dependents and designated beneficiaries of employment-related benefits through SPE.

176. Plaintiffs further request that the Court order SPE to (1) identify and notify all members of the class who have not yet been informed of the Data Breach;

and (2) notify affected current and former employees of any future data breaches by email within 24 hours of SPE's discovery of a breach or possible breach and by mail within 72 hours.

177. As a result of SPE's violations of Civil Code sections 1798.81.5 and 1798.82, Plaintiffs and members of the California Class have incurred and will incur damages, including but not necessarily limited to: (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to SPE for the purpose of deriving employment from SPE and with the understanding that SPE would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, publication, and/or theft of their PII and the PII of their family members and designated beneficiaries of employment-related benefits through SPE; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity and health care/medical data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets; (7) unauthorized use of compromised PII to open new financial and/or health care or medical accounts;

(8) tax fraud and/or other unauthorized charges to financial, health care or medical accounts and associated lack of access to funds while proper information is confirmed and corrected; (9) the continued risk to their PII, and the PII of their family members and designated beneficiaries of employment-related benefits through SPE, which remain in SPE's possession and are subject to further breaches so long as SPE fails to undertake appropriate and adequate measures to protect the PII in its possession; and (10) future costs in terms of time, effort and money that will be expended, to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of the California Class members, their families, and their designated beneficiaries of employment-related benefits through SPE.

178. Plaintiffs seek all remedies available under Civil Code section 1798.84, including actual and statutory damages, equitable relief, and reasonable attorneys' fees. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

COUNT IV: Violation of California Confidentiality of Medical Information Act California Civil Code § 56 *et seq*.

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

180. Plaintiffs bring this cause of action on behalf of the Nationwide Class.

181. California's Confidentiality of Medical Information Act ("CMIA"), Cal. Civ. Code § 56, *et seq*., requires employers like SPE to protect their employees'

confidential medical information and not release private medical information without signed proper authorization.

182. The CMIA defines "medical information" as "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment." The CMIA defines "individually identifiable" as "medical information [that] includes or contains any element of personal identifying information sufficient to allow identification of the individual, such as the patient's name, address, electronic mail address, telephone number, or Social Security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity."

183. SPE has violated section 56.20(a) of the CMIA, which requires an "employer who receives medical information [to] establish appropriate procedures to ensure the confidentiality and protection from unauthorized use and disclosure of that information." The procedures the employer must establish "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." SPE violated section 56.20(a) of the CMIA by failing to maintain the confidentiality of class members' medical information and by

failing to institute reasonable safeguards to protect their medical information from disclosure.

184. SPE also violated section 56.36(b) of the CMIA by negligently releasing Plaintiffs' and class members' medical information.

185. SPE did not obtain Plaintiffs' or class members' written authorization to disclose or release their medical information.

186. As a result of the Data Breach, class members' medical information has been posted to the internet where it has been viewed by members of the media and the public. This medical information includes complaints from employees about unpaid medical insurance claims, spreadsheets that contained the health conditions and medical procedures for employees for diagnoses such as cancer, heart disorders, and end-stage renal disease, along with employees' PII that was contained in the spreadsheets and other data released in the breach.

187. SPE has admitted that the personal information exposed by the Data Breach included "HIPAA protected health information, such as name, Social Security number, claims appeals information you submitted to SPE (including diagnosis and disability code), date of birth, home address, and member ID number to the extent that you and/or your dependents participated in SPE health plans," as well as "health/medical information that [employees] provided to [SPE] outside of SPE health plans."

188. Among other things, SPE is and was negligent in failing to maintain its current and former employees' medical information in encrypted form; failing to use reasonable security procedures to prevent unauthorized access to files containing the medical information; failing to use reasonable authentication procedures so that the medical information could be tracked in case of a security breach; delaying notifying its current and former employees that their private medical information had been compromised; and allowing unauthorized access to employees' private medical files, all in violation of the CMIA and HIPAA.

189. Plaintiffs request that the Court enter an injunction requiring SPE to implement and maintain reasonable security procedures to protect its employees' medical information in compliance with the CMIA, including, but not limited to, ordering that SPE: (1) engage third party security auditors/penetration testers as well as internal security personnel to conduct testing consistent with prudent industry practices, including simulated attacks, penetration tests, and audits on SPE's systems on a periodic basis; (2) engage third party security auditors and internal personnel, consistent with prudent industry practices, to run automated security monitoring – particularly for employees' medical information – consistent with prudent industry practices; (3) audit, test, and train its security personnel regarding any new or modified procedures designed to protect employees' medical information; (4) purge, delete and destroy, in a secure manner, employees' medical information not necessary for its business operations; (5) conduct regular database scanning and

securing checks, consistent with prudent industry practices; (6) periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach, consistent with prudent industry practices; (7) receive periodic compliance audits by a third party regarding the security of the computer systems SPE uses to store the personal information of its current and former employees; (8) meaningfully educate its current and former employees about the threats they face as a result of the loss of their personal information to third parties, as well as the steps they must take to protect themselves; and (9) provide ongoing identity theft protection, monitoring, and recovery services to Plaintiffs and class members, as well as their dependents and designated beneficiaries of employment-related benefits through SPE.

190. Plaintiffs also seek an award of $1,000 in statutory damages for each class member pursuant to section 56.36(b)(1) of the CMIA. An award of statutory damages is necessary to deter future violations by SPE and other employers.

191. Plaintiffs also seek actual damages pursuant to section 56.36(b)(2). As a result of SPE's violation of the CMIA, Plaintiffs and class members have incurred and will incur damages, including but not necessarily limited to: (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to SPE for the purpose of deriving employment from SPE and with the understanding that SPE would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, publication, and/or theft

of their PII and the PII of their family members and designated beneficiaries of employment-related benefits through SPE; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity and health care/medical data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets; (7) unauthorized use of compromised PII to open new financial and/or health care or medical accounts; (8) tax fraud and/or other unauthorized charges to financial, health care or medical accounts and associated lack of access to funds while proper information is confirmed and corrected; (9) the continued risk to their PII, and the PII of their family members and designated beneficiaries of employment-related benefits through SPE, which remain in SPE's possession and are subject to further breaches so long as SPE fails to undertake appropriate and adequate measures to protect the PII in its possession; and (10) future costs in terms of time, effort and money that will be expended, to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of the Nationwide Class members, their

families, and their designated beneficiaries of employment-related benefits through SPE.

192. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

COUNT V: Violation of the Unfair Competition Law
California Business and Professions Code Section 17200 *et seq*.

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

194. Plaintiffs bring this cause of action on behalf of the Nationwide Class.

195. SPE engaged in unlawful, unfair, and fraudulent business practices in violation of the Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*. ("UCL").

196. SPE's acts, omissions and conduct constitute unlawful, unfair, and fraudulent business practices under the UCL.

197. SPE's acts, omissions and conduct were unlawful because they violated the California Customer Records Act, the CMIA, and HIPAA, and because they were negligent.

198. SPE's practices were unlawful and in violation of Civil Code section 1798.81.5(b) because SPE failed to take reasonable security measures in protecting its current and former employees' PII.

199. SPE's practices were also unlawful and in violation of California Civil Code section 1798.82 because SPE unreasonably delayed informing Plaintiffs and class members about the breach of security after SPE knew the Data Breach occurred.

200. SPE's practices were unlawful and in violation of section 56.20 of the CMIA because it did not establish proper procedures to secure the confidentiality of its current and former employees' medical information.

201. SPE's practices were also unlawful and in violation of section 56.36(b) of the CMIA because SPE negligently released Plaintiffs' and class members' medical information that was within SPE's control.

202. SPE's practices were also unlawful and in violation of HIPAA because SPE failed to establish procedures to keep employees' medical information confidential and private.

203. SPE's acts, omissions and conduct constitute a violation of the unlawful prong of the UCL because SPE failed to comport with a reasonable standard of care and public policy as reflected in statutes like the Information Practices Act of 1977, HIPAA, the CMIA, and the California Customer Records Act, which were enacted to protect individuals' personal information and ensure that entities that solicit or are entrusted with personal information use reasonable security measures.

204. In unduly delaying informing Plaintiffs and the class members of the Data Breach, SPE engaged in unfair business practices by engaging in conduct that undermines or violates the stated policies underlying the California Customer

Records Act and other privacy statutes. In enacting the California Customer Records Act, the Legislature stated that "[i]dentity theft is costly to the marketplace and to consumers" and that "victims of identity theft must act quickly to minimize the damage; therefore expeditious notification of possible misuse of a person's personal information is imperative." 2002 Cal. Legis. Serv. Ch. 1054 (A.B. 700) (WEST). SPE's conduct also undermines California public policy as reflected in other statutes such as the Information Practices Act of 1977, which was enacted to protect individuals' data and ensure that entities who solicit or are entrusted with personal data use reasonable security measures.

205. SPE's acts, omissions, and conduct also constitute "unfair" business acts or practices because they offend public policy and constitute immoral, unethical, and unscrupulous activities that caused substantial injury, including to Plaintiffs and class members. The gravity of harm resulting from SPE's conduct outweighs any potential benefits attributable to the conduct and there were reasonably available alternatives to further SPE's legitimate business interests. SPE's conduct also undermines public policy as reflected in statutes like the Information Practices Act of 1977, Cal. Civ. Code § 1798, *et seq*., HIPAA, the CMIA, and the California Customer Records Act, which were enacted to protect individuals' personal data and ensure that entities who solicit or are entrusted with personal data use reasonable security measures.

206. SPE has engaged in fraudulent business practices by making material misrepresentations and by failing to disclose material information regarding SPE's

deficient security policies and practices, the security of the PII of Plaintiffs and class members, and the Data Breach.

207. SPE had exclusive knowledge of material information regarding its deficient security policies and practices, and regarding the security of the PII of Plaintiffs and class members. This exclusive knowledge includes, but is not limited to, information that SPE received through internal and other non-public audits and reviews that concluded that SPE's security policies were substandard and deficient, and that the PII of Plaintiffs and class members and other SPE data was vulnerable as a result. This exclusive knowledge also includes information regarding SPE's data security, not reported publicly, that SPE received in connection with data breaches at SPE and other Sony companies that occurred over the years. SPE also had exclusive knowledge concerning the measures, or lack thereof, that SPE took in response to the data breaches that have occurred over the years at SPE and other Sony companies and in response to the various audits that have reflected security gaps at SPE and other Sony companies.

208. SPE also had exclusive knowledge about the extent of the Data Breach, including during the days and weeks following the Data Breach.

209. SPE also had exclusive knowledge about the length of time that it maintained former employees' PII after they left SPE's employment.

210. SPE failed to disclose, and actively concealed, the material information it had regarding SPE's deficient security policies and practices, and regarding the

security of the PII of Plaintiffs and class members. For example, even though SPE has long known, through internal audits and otherwise, that its security policies and practices were substandard and deficient, and that the PII of Plaintiffs and class members was vulnerable as a result, SPE failed to disclose this information to, and actively concealed this information from, Plaintiffs, class members and the public. SPE also did not disclose, and actively concealed, information regarding the extensive length of time that it maintains former employees' PII and other records. Likewise, in the days and weeks following the Data Breach, SPE failed to disclose, and actively concealed, information that it had regarding the extent and nature of the Data Breach.

211. SPE also has made material affirmative misrepresentations about SPE's security policies and practices and the security of the PII of Plaintiffs and class members. For example, following the 2011 PSN data breach, Sony President Kazuo Hirai indicated that, after that breach, Sony had "basically … done everything to bring our practices at least in line with industry standards or better." In fact, contrary to this representation, Sony failed to invest the resources necessary to bring the security practices at the Sony companies in line with industry standards.

212. SPE had a duty to disclose the material information that it had because, *inter alia*, it had exclusive knowledge of the information, it actively concealed the information, it made affirmative statements that were inconsistent with the information it did not disclose, and because SPE was in a fiduciary position vis-à-vis

Plaintiffs and class members by virtue of the fact that SPE collected and maintained their financial information, medical information, and other PII.

213. SPE's misrepresentations and omissions were material, misleading, and had a tendency to deceive.

214. Plaintiffs were misled by SPE's misrepresentations and omissions about SPE's data security, and they reasonably relied upon them to their detriment. But for SPE's misrepresentations and omissions, Plaintiffs would not have provided the PII that they provided to SPE (regarding themselves and their family members) and would have insisted that their PII be more securely protected and removed from SPE's systems promptly after their employment ended. They also would have taken additional steps to protect their identities and to protect themselves from the sort of harm that could flow from SPE's lax security measures. But for SPE's misrepresentations and omissions, Plaintiffs would not be experiencing identity theft, identity fraud, and/or the increased risk of harm they are now facing, as a result of the Data Breach. But for the fact that SPE sat on information regarding the Data Breach, rather than immediately disclosing it, Plaintiffs would have taken more immediate steps to protect their identities and they would have been able to minimize the harm they have suffered as a result of the Data Breach.

215. As a direct and proximate result of SPE's unlawful, unfair, and fraudulent business practices as alleged herein, Plaintiffs and members of the class have suffered injury in fact. Plaintiffs and the class have been injured in that their

personal, financial, and medical PII has been compromised, subject to identity theft, identity fraud, and/or is at risk for future identity theft and fraudulent activity on their financial accounts. Class members have also lost money and property that would not have be lost but for SPE's unlawful and unfair conduct.

216. As a direct and proximate result of SPE's unlawful, unfair, and fraudulent business practices as alleged herein, Plaintiffs and class members already suffer from identity theft, identity and financial fraud, and/or a continuing increased risk of identity theft and identity, financial and medical fraud due to the compromise, publication, and/or unauthorized use of their financial, health care, and/or medical PII. Plaintiffs have also been injured by, among other things: (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to SPE for the purpose of deriving employment from SPE and with the understanding that SPE would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, publication, and/or theft of their PII and the PII of their family members and designated beneficiaries of employment-related benefits through SPE; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity and health

care/medical data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets; (7) unauthorized use of compromised PII to open new financial and/or health care or medical accounts; (8) tax fraud and/or other unauthorized charges to financial, health care or medical accounts and associated lack of access to funds while proper information is confirmed and corrected; (9) the continued risk to their PII, and the PII of their family members and designated beneficiaries of employment-related benefits through SPE, which remain in SPE's possession and are subject to further breaches so long as SPE fails to undertake appropriate and adequate measures to protect the PII in its possession; and (10) future costs in terms of time, effort and money that will be expended, to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of the Nationwide Class members, their families, and their designated beneficiaries of employment-related benefits through SPE.

217. As a result of SPE's violations of the UCL, Plaintiffs and members of the class are entitled to injunctive relief, including, but not limited to an order that SPE: (1) engage third party security auditors/penetration testers as well as internal security personnel to conduct testing consistent with prudent industry practices, including simulated attacks, penetration tests, and audits on SPE's systems on a periodic basis; (2) engage third party security auditors and internal personnel to run

automated security monitoring consistent with prudent industry practices; (3) audit, test, and train its security personnel regarding any new or modified procedures; (4) purge, delete and destroy, in a secure manner, employee data not necessary for its business operations; (5) conduct regular database scanning and securing checks consistent with prudent industry practices; (6) periodically conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach consistent with prudent industry practices; (7) receive periodic compliance audits by a third party regarding the security of the computer systems SPE uses to store the PII of its current and former employees; (8) meaningfully educate its current and former employees about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves; and (9) provide ongoing identity theft protection, monitoring, and recovery services, to Plaintiffs and class members, as well as their dependents and designated beneficiaries of employment-related benefits through SPE.

218. Because of SPE's unlawful, unfair, and fraudulent business practices, Plaintiffs and the class are entitled to relief, including attorneys' fees and costs, restitution, declaratory relief, and a permanent injunction enjoining SPE from its unlawful and unfair practices. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

COUNT VI: Declaratory Judgment

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

220. As previously alleged, Plaintiffs and the Nationwide Class have stated claims against SPE based on negligence and implied contract.

221. SPE has failed to live up to its obligations to provide reasonable security measures for the PII of Plaintiffs and the Nationwide Class, as indicated by its corporate history of security breaches and the specific Data Breach that precipitated this lawsuit.

222. In addition, the Data Breach has rendered SPE's system even more vulnerable to unauthorized access and requires that SPE immediately take even more stringent measures to currently safeguard the PII of Plaintiffs and the Nationwide Class going forward.

223. An actual controversy has arisen in the wake of SPE's Data Breach regarding SPE's *current* obligations to provide reasonable data security measures to protect the PII of Plaintiffs and the Nationwide Class. On information and belief, SPE maintains that its security measures were, and remain, reasonably adequate. On information and belief, SPE further denies that it previously had or now has any obligation to better safeguard the PII of Plaintiffs and the Nationwide Class.

224. Plaintiffs thus seek a declaration that to comply with its existing obligations, SPE must implement specific additional, prudent industry security

practices, as outlined below, to provide reasonable protection and security to the PII of Plaintiffs and the Nationwide Class.

225. Specifically, Plaintiffs and the class seek a declaration that (a) SPE's existing security measures do not comply with its obligations, and (b) that to comply with its obligations, SPE must implement and maintain reasonable security measures on behalf of Plaintiffs and the Nationwide Class, including, but not limited to: (1) engaging third party security auditors/penetration testers as well as internal security personnel to conduct testing consistent with prudent industry practices, including simulated attacks, penetration tests, and audits on SPE's systems on a periodic basis; (2) engaging third party security auditors and internal personnel to run automated security monitoring consistent with prudent industry practices; (3) auditing, testing, and training its security personnel regarding any new or modified procedures; (4) purging, deleting and destroying, in a secure manner, employee data not necessary for its business operations; (5) conducting regular database scanning and securing checks consistent with prudent industry practices; (6) periodically conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach consistent with prudent industry practices; (7) receiving periodic compliance audits by a third party regarding the security of the computer systems SPE uses to store the personal information of its current and former employees; (8) meaningfully educating its current and former employees about the threats they face as a result of the loss of

their PII to third parties, as well as the steps they must take to protect themselves; and (9) providing ongoing identity theft protection, monitoring, and recovery services to Plaintiffs and class members, as well as their dependents and designated beneficiaries of employment-related benefits through SPE.

COUNT VII: Violation of Virginia Code Annotated § 18.2-186.6

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

227. Plaintiffs Corona and Springer bring this cause of action on behalf of the Virginia Class.

228. SPE is an "entity" as defined by section 18.2-186.6(A).

229. Plaintiffs Corona and Springer and class members are "individuals" as defined by section 18.2-186.6(A).

230. The PII of current and former SPE employees that was compromised and exposed in the Data Breach constitutes "personal information" as defined by section 18.2-186.6(A), which includes Social Security numbers, driver's license numbers, financial account numbers, and credit and debit card numbers in combination with security codes, access codes, or passwords that permit access to financial accounts.

231. The breach of the PII of thousands of current and former SPE employees was a "breach of the security system" of SPE as defined by section 18.2-186.6(A).

232. Under section 18.2-186.6(B), SPE was required to disclose any breach of the security of its system following discovery or notification of the breach to the

Office of the Attorney General and any affected resident of the Commonwealth of Virginia without unreasonable delay.

233. In violation of section 18.2-186.6(B), SPE unreasonably delayed informing Virginia Class members about the breach of their personal information, and failed to disclose to Virginia Class members without unreasonable delay that their unencrypted, or not properly and not securely encrypted, personal information had been breached.

234. Upon information and belief, no law enforcement agency instructed SPE that notification to Virginia Class members would impede an investigation.

235. As a result of SPE's violation of section 18.2-186.6, Virginia Class members have incurred and will incur economic damages to money or property, including but not necessarily limited to: (1) the diminution in the value of their PII entrusted to SPE for the purpose of deriving employment from SPE and with the understanding that SPE would safeguard their PII against theft and not allow access and misuse of their PII by others; (2) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts; (3) lost opportunity costs associated with effort extended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity and health care/medical data misuse; (4) costs associated with the ability to use credit and assets

frozen or flagged due to credit misuse, including increased costs to use credit, credit scores, credit reports and assets; and (5) tax fraud and/or other unauthorized charges to financial, health care or medical accounts and associated lack of access to funds while proper information is confirmed and corrected.

236. Plaintiffs further request that the Court order SPE to (1) identify and notify all members of the class who have not yet been informed of the Data Breach; and (2) notify affected current and former employees of any future data breaches by email within 24 hours of SPE's discovery of a breach or possible breach and by mail within 72 hours.

237. Plaintiffs Corona and Springer, individually and on behalf of the Virginia Class, seek all remedies available under section 18.2-186.6, including but not limited to damages and equitable relief. Plaintiffs also seek reasonable attorneys' fees and costs under applicable law including Federal Rule of Civil Procedure 23 and California Code of Civil Procedure § 1021.5.

Count VIII: Violation of Colorado Revised Statutes Annotated § 6-1-716

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

239. Plaintiff Forster brings this cause of action on behalf of the Colorado Class.

240. SPE is a "commercial entity" as defined in section 6-1-716(1)(b).

241. The PII of current and former SPE employees that was compromised and exposed in the Data Breach constitutes "personal information" as defined by section 6-1-716(1)(d), which includes Social Security numbers, driver's license numbers, account numbers or credit or debit card numbers, in combination with any required security code, access code, or password that would permit access to a resident's financial account.

242. The breach of the PII of thousands of current and former SPE employees was a "breach of the security of the system" of SPE as defined by section 6-1-716(1)(a).

243. SPE violated section 6-1-716(2) through its unreasonable delay in informing Colorado Class members about the breach of their personal information, and failure to disclose to Colorado Class members without unreasonable delay that their unencrypted, or not properly and not securely encrypted, personal information had been breached.

244. Upon information and belief, no law enforcement agency instructed SPE that notification to Colorado Class members would impede a criminal investigation.

245. As a result of SPE's violation of section 6-1-716, Colorado Class members have incurred and will incur economic damages, including but not necessarily limited to: (1) the diminution in the value of their PII entrusted to SPE for the purpose of deriving employment from SPE and with the understanding that SPE would safeguard their PII against theft and not allow access and misuse of their PII

by others; (2) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts; (3) lost opportunity costs associated with effort extended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity and health care/medical data misuse; (4) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including increased costs to use credit, credit scores, credit reports and assets; and (5) tax fraud and/or other unauthorized charges to financial, health care or medical accounts and associated lack of access to funds while proper information is confirmed and corrected.

246. Plaintiffs further request that the Court order SPE to (1) identify and notify all members of the Colorado Class who have not yet been informed of the Data Breach; and (2) notify affected current and former employees of any future data breaches by email within 24 hours of SPE's discovery of a breach or possible breach and by mail within 72 hours.

247. Plaintiff Forster, individually and on behalf of the Colorado Class, seeks all remedies available under section 6-1-716, including but not limited to damages and equitable relief, and reasonable attorneys' fees and costs under applicable law.

IX. PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and on behalf of the proposed classes, request that the Court:

a. Certify this case as a class action, appoint Plaintiffs as class representatives, and appoint Plaintiffs' counsel to represent the classes;

b. Find that SPE breached its duty to safeguard and protect the PII of Plaintiffs and the class members that was compromised in the Data Breach;

c. Award Plaintiffs and class members appropriate relief, including actual and statutory damages, restitution and disgorgement;

d. Award equitable, injunctive and declaratory relief as may be appropriate;

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

f. Award pre-judgment and post-judgment interest as prescribed by law; and

g. Grant additional legal or equitable relief as this Court may find just and proper.

X. JURY TRIAL DEMANDED

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

Dated: March 2, 2015

Respectfully submitted,

KELLER ROHRBACK L.L.P.

By: */s/ Lynn Lincoln Sarko*
Lynn Lincoln Sarko, *Admitted pro hac vice*
lsarko@kellerrohrback.com
Gretchen Freeman Cappio, *Admitted pro hac vice*
gcappio@kellerrohrback.com
Cari Campen Laufenberg, *Admitted pro hac vice*
claufenberg@kellerrohrback.com
1201 Third Avenue, Suite 3200
Seattle, WA 98101
Telephone: (206) 623-1900
Facsimile: (206) 623-3384

Matthew J. Preusch
mpreusch@kellerrohrback.com
KELLER ROHRBACK L.L.P.
1129 State Street, Suite 8
Santa Barbara, CA 93101
Telephone: (805) 456-1496
Facsimile: (805) 456-1497

Proposed Interim Co-Lead Class Counsel and Liaison Counsel

Daniel C. Girard
dcg@girardgibbs.com
Amanda M. Steiner
as@girardgibbs.com
Linh G. Vuong
lgv@girardgibbs.com
GIRARD GIBBS LLP
601 California Street, 14th Floor
San Francisco, CA 94108
Telephone: (415) 981-4800
Facsimile: (415) 981-4846

Michael W. Sobol
msobol@lchb.com

RoseMarie Maliekel
rmaliekel@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: (415) 956-1000
Facsimile: (415) 956-1008

Nicholas Diamand
ndiamand@lchb.com
LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
250 Hudson Street, 8th Floor
New York, NY10013-1413
Telephone: (212) 355-9500
Facsimile: (212) 355-9592

Proposed Interim Co-Lead Class Counsel

Hank Bates
hbates@cbplaw.com
Allen Carney
acarney@cbplaw.com
David Slade
dslade@cbplaw.com
CARNEY BATES & PULLIAM, PLLC
11311 Arcade Drive
Little Rock, AR 72212
Telephone: (501) 312-8500
Facsimile: (501) 312-8505

Raúl Pérez
Raul.Perez@Capstonelawyers.com
Jordan L. Lurie
Jordan.Lurie@capstonelawyers.com
Robert Friedl
Robert.Friedl@capstonelawyers.com
Tarek H. Zohdy
Tarek.Zohdy@capstonelawyers.com
Cody R. Padgett
Cody.Padgett@capstonelawyers.com

CAPSTONE LAW APC
1840 Century Park East, Suite 450
Los Angeles, CA 90067
Telephone: (310) 556-4811
Facsimile: (310) 943-0396

John H. Gomez
john@gomeztrialattorneys.com
John P. Fiske
jfiske@gomeztrialattorneys.com
Deborah Dixon
ddixon@gomeztrialattorneys.com
GOMEZ TRIAL ATTORNEYS
655 West Broadway, Suite 1700
San Diego, CA 92101
Telephone: (619) 237-3490
Facsimile: (619) 237-3496

Joseph G.Sauder
jgs@chimicles.com
Matthew D. Schelkopf
mds@chimicles.com
Benjamin F. Johns
bfj@chimicles.com
Joseph B. Kenney
jbk@chimicles.com
CHIMICLES & TIKELLIS LLP
One Haverford Centre
361 West Lancaster Avenue
Haverford, PA 19041
Telephone: (610) 642-8500
Facsimile: (610) 649-3633

Richard A. Maniskas, Esquire
rmaniskas@rmclasslaw.com
RYAN & MANISKAS, LLP
995 Old Eagle School Road, Suite 311
Wayne, PA 19087
Telephone: (484) 588-5516
Facsimile: (484) 450-2582

Steven M. Tindall
stindall@rhdtlaw.com
Valerie Bender
vbrender@rhdtlaw.com
RUKIN HYLAND DORIA & TINDALL LLP
100 Pine Street, Suite 2150
San Francisco, CA 94111
Telephone: (415) 421-1800
Facsimile: (415) 421-1700

Katrina Carroll
kcarroll@litedepalma.com
Kyle A. Shamberg
kshamberg@litedepalma.com
LITE DEPALMA GREENBERG, LLC
211 W. Wacker Drive, Suite 500
Chicago, IL 60613
Telephone: (312) 750-1265
Facsimile: (312) 212-5919

Additional Plaintiffs' Counsel

CERTIFICATE OF SERVICE

I, Lynn Lincoln Sarko, hereby certify that on March 2, 2015 I electronically filed **AMENDED CLASS ACTION COMPLAINT** with the Clerk of the United States District Court for the Central District of California using the CM/ECF system, which shall send electronic notification to all counsel of record.

/s/ Lynn Lincoln Sarko
Lynn Lincoln Sarko