

KELLER GROVER LLP
1965 Market Street, San Francisco, CA 94103
Tel. 415.543.1305 | Fax. 415.543.7861

Eric A. Grover, Esq. (SBN 136080)
eagrover@kellergrover.com
Robert W. Spencer (SBN 238491)
rspencer@kellergrover.com
KELLER GROVER LLP
1965 Market Street
San Francisco, California 94103
Telephone: (415) 543-1305
Facsimile: (415) 543-7861

Attorneys for Plaintiff
RUSSELL ASHLOCK

**SUPERIOR COURT OF THE STATE OF CALIFORNIA
IN AND FOR THE COUNTY OF SAN FRANCISCO**

RUSSELL ASHLOCK, on behalf of)
himself, and all others similarly situated,)
)
Plaintiff,)
)
v.)
)
SUNRUN INC.; SUNRUN)
INSTALLATION SERVICES INC.; and)
DOES 1 through 10, inclusive,)
)
Defendants.)

Case No.: **CGC-17-557027**

CLASS ACTION COMPLAINT FOR:

1. NEGLIGENCE;
2. VIOLATIONS OF THE BUSINESS & PROFESSIONS CODE;
3. DECLARATORY RELIEF; AND
4. BREACH OF CONTRACT

DEMAND FOR JURY TRIAL

BY FAX
ONE LEGAL LLC

Russell Ashlock ("Plaintiff"), individually and on behalf of all others similarly situated, files this Class Action Complaint against SUNRUN INC. and SUNRUN INSTALLATION SERVICES INC. (collectively "Defendants" or "Sunrun") and alleges the following based on personal knowledge, the investigation of counsel, and information and belief.

INTRODUCTION

1. Plaintiff and the other putative class members are current and former employees of Defendants who entrusted their personally identifiable information ("PII") to Sunrun. Defendants betrayed Plaintiff's and class members' trust by failing to properly safeguard and protect their PII and negligently disclosed their PII to cybercriminals.

2. Sunrun has informed current and former employees that, in January 2017, it learned that a Sunrun employee had responded to an Internet "phishing"¹ scam by forwarding to unknown cybercriminals the 2016 Form W-2's for many, if not all, of Defendants' current and former employees (collectively, "Employees"). The Form W-2 data contained sensitive personally identifying PII, including, among other things, names, addresses, wage information and, most importantly, Social Security numbers. By disclosing its Employees' PII to cybercriminals (the "Data Breach"), Sunrun put all of its Employees at risk.

3. Prior to the Data Breach, Defendants made a concerted effort to reduce the number of employees who had access to the PII that was compromised because of the fear of such data being compromised.

4. Based on what has happened in connection with similar W-2 data breaches, it is believed that almost immediately after the Data Breach, the cybercriminals who exploited Sunrun's wrongful actions have started filing fraudulent federal and state tax returns in the names of Employees.

¹ "Phishing" is an attempt to acquire PII by masquerading as a trustworthy entity through an electronic communication. See <http://www.onguardonline.gov/articles/0003-phishing>. Phishing is typically carried out by e-mail spoofing that looks like a legitimate email and often directs the recipient to provide PII. When criminals have access to PII from a large group of similarly situated victims, it is much more feasible to develop a believable phishing spoof email.

1 5. Sunrun negligently failed to take the necessary precautions required to safeguard
2 and protect Plaintiff's and class members' PII from unauthorized disclosure resulting in the PII of
3 Plaintiff and class members being turned over to cybercriminals. Defendants actions represent a
4 flagrant disregard of Plaintiff's and class members' rights, both as to privacy and property.

5 6. Employees are now, and for the rest of their lives will be, at a heightened risk of
6 identity theft. As a direct result of the Data Breach, many Employees likely have already, and
7 will suffer in the future, out-of-pocket costs attempting to rectify fraudulent tax returns and
8 engaging services to monitor and protect their identity and credit. Employees will continue to
9 suffer out-of-pocket costs in the future to protect and, if necessary, repair their credit and identity.
10 By this action, Plaintiff seeks to hold Sunrun responsible for the harm caused by its negligence.

11 7. Plaintiff brings this action because, as a direct and/or proximate result of
12 Defendants wrongful actions and/or inaction and the resulting Data Breach, Plaintiff has incurred
13 (and will continue to incur) damages in the form of, *inter alia*, (i) loss of privacy and/or (ii) the
14 additional damages set forth in detail below, which are incorporated herein by reference.

15 8. As a direct and/or proximate result of Defendants wrongful actions and/or inaction
16 and the resulting Data Breach, Plaintiff and the other class members have been deprived of the
17 value of their PII, for which there is a well-established national and international market. For
18 example, stolen PII is sold on the cyber black market for \$14 to \$25 per record to individuals
19 focused on committing fraud or needing or wanting a new identity.

20 9. Defendants' wrongful actions and/or inaction and the resulting Data Breach have
21 also placed Plaintiff and the other class members at an imminent, immediate and continuing
22 increased risk of identity theft and identity fraud. Javelin Strategy & Research ("Javelin"), a
23 leading provider of quantitative and qualitative research, released its 2015 Identity Fraud Report
24 ("the Javelin Report"), quantifying the impact of data breaches. According to the Javelin Report,
25 individuals whose PII is subject to a reported data breach are approximately 9.5 times more likely
26 than the general public to suffer identity fraud and/or identity theft. Moreover, there is a high
27 likelihood that significant identity fraud and/or identity theft has not yet been discovered or
28

1 reported, and a high probability that criminals who may now possess Plaintiff's and the other
2 class members' PII and not yet used the information will do so at a later date or re-sell it.

3 10. Plaintiff on behalf of himself and the other class members, seeks actual damages,
4 economic damages, injunctive relief, and attorneys' fees, litigation expenses, and costs.

5 JURISDICTION AND VENUE

6 11. This Court has personal jurisdiction over the parties because, at all relevant times,
7 Plaintiff was a California resident who worked in California for Defendant and Defendant has
8 systematically and continuously conducted business in the State of California.

9 12. Venue is proper in this Court under California Code of Civil Procedure § 395.5
10 because each Defendant's principal place of business is located within San Francisco County at
11 595 Market Street, 29th Floor, San Francisco California 94105.

12 PARTIES

13 13. Plaintiff RUSSELL ASHLOCK is a resident of California and a former employee
14 of Defendants. Plaintiff Ashlock found about the data breach after reading about it on the internet
15 in early February 2017. He then contacted Sunrun and was informed that Sunrun had disclosed
16 his Form W-2 in the data breach. He also received a letter on February 6, 2017 from Sunrun that
17 informed him that Sunrun had disclosed his Form W-2 in the data breach. Plaintiff Ashlock
18 learned that someone had filed a false tax return using his information on January 29, 2017.

19 14. Defendant Sunrun Inc. is a corporation organized under the laws of the state of
20 Delaware with its principal place of business in San Francisco, California.

21 15. Defendant Sunrun Installation Services Inc. is a corporation organized under the
22 laws of the state of Delaware with its principal place of business in San Francisco, California.

23 FACTUAL ALLEGATIONS

24 16. Data security breaches – and data security breach litigation – dominated the
25 headlines in 2015 and 2016. Continuous widely publicized breaches have led to 30,000 articles a
26
27
28

1 month being published that reference data breach litigation. Law firms have collectively
2 published more than 156,000 articles on the topic.²

3
4 17. According to the Privacy Rights Clearinghouse Chronology of Data Breaches, 282
5 breaches were publicly reported during the fourth quarter of 2014 through the fourth quarter of
6 2015.³

7 18. Sunrun's own website Privacy Policy recognizes the critical importance of data
8 security, stating:

9 We have implemented measures designed to secure your personal
10 information from accidental loss and from unauthorized access, use, alteration
11 and disclosure. All information you provide to us is stored on secure servers
12 behind firewalls by our third party cloud computing services providers. Any
13 payment transactions are also conducted via secure third party web-based
14 payment portals.

15 The safety and security of your information also depends on you. Where we
16 have given you (or where you have chosen) a password for access to certain parts
17 of our Website, you are responsible for keeping this password confidential. We
18 ask you not to share your password with anyone. We urge you to be careful about
19 giving out information in public areas of the Website. The information you share
20 in public areas may be viewed by any user of the Website.⁴

21 19. Sunrun announced that, on or about January 20, 2017, it discovered that it was the
22 victim of a "phishing" scam (the "Data Breach"). According to Sunrun, the Data Breach resulted
23 in the release of PII for current and former employees.⁵ In the Data Breach, Sunrun provided to
24 unknown cybercriminals the 2016 Forms W-2 data for some if not all, of its Employees. The

25 ² Google News Search for "Data Breach Litigation" conducted on March 22, 2016 (covers 30
26 days); Lexology.com search for "Data Breach Litigation" conducted on March 25, 2016.

27 ³ See Privacy Rights Clearinghouse Chronology of Breaches available at
28 <http://www.privacyrights.org>.

⁴ <https://www.sunrun.com/privacy-policy>

⁵ <http://www.sfgate.com/business/article/Sunrun-hack-nabs-employee-W-2-tax-forms-10889441.php>

1 Form W-2 data disclosed the Employees' names, addresses, compensation and, most importantly,
2 Social Security numbers.

3 20. The cybercriminals who obtained the Employees' PII have and may continue to
4 exploit the data themselves and/or sell the data in the so-called "dark markets." Having obtained
5 the Employees' names, addresses, compensation, and Social Security numbers, cybercriminals
6 can pair the data with other available information to commit a broad range of fraud in an
7 Employee's name, including but not limited to:

- 8 a. obtaining employment;
- 9 b. obtaining a loan;
- 10 c. applying for credit cards or spending money;
- 11 d. filing false tax returns;
- 12 e. obtaining medical care;
- 13 f. stealing Social Security and other government benefits; and
- 14 g. applying for a driver's license, birth certificate or other public document.

15 21. In addition, if an Employee's Social Security number is used to create a false
16 identification for someone who commits a crime, the Employee may become entangled in the
17 criminal justice system, impairing the Employee's ability to gain employment or obtain a loan.

18 22. For the rest of their lives, Plaintiff and class members will bear an immediate and
19 heightened risk of all manners of identity theft.

20 23. By the time current and former employees received notice of the Data Breach, it is
21 believed that many were already the victims of identity theft, including the filing of fraudulent tax
22 returns.

23 24. W-2 phishing schemes are not new. In 2016, Internet security researcher Brian
24 Krebs warned of this precise scam on his Internet website. Krebs warned that as the 2016 tax
25 season approached Internet scammers were trying to scam various companies by sending false
26
27
28

1 emails, purportedly from the company's chief executive officer, to individuals in the human
2 resources and accounting departments and asking for copies of Forms W-2 data.⁶

3 25. Sunrun has already conceded its fault in the Data Breach. Sunrun's Chief
4 Executive Officer wrote in an email to employees: "On Friday, January 20, a targeted email from
5 a scammer impersonating me was sent to our payroll department requesting employee W-2s.
6 Unfortunately, the phishing email wasn't recognized for what it was -- a scam -- and employee W-
7 2s for 2016 were disclosed externally. These W-2 forms include your name, address, Social
8 Security number, salary, and taxes withheld for 2016."

9 **Sunrun's Current and Former Employees Have Suffered Concrete Injury**

10 26. As part of their employment, the Employees were required to provide Sunrun with
11 sensitive personal information, including their Social Security numbers. Sunrun had a duty to
12 protect that information against wrongful disclosure to third parties. Sunrun failed to comply
13 with its duties to its current and former employees by failing to implement policies and
14 procedures to prevent cybercriminals and scammers from obtaining Employees' PII.

15 27. On information and belief, as a result of the Data Breach, numerous Employees
16 have already suffered damages. In addition, the disclosure of an individual's Social Security
17 number puts one at great risk of future fraudulent conduct. By pairing a Social Security number
18 with someone's name, address, compensation and, perhaps, other readily available information,
19 an identity thief can commit a broad range of fraud, including but not limited to a) obtaining
20 unemployment; b) obtaining a loan; c) applying for credit cards or spending money under the
21 victim's name; d) filing false tax returns; e) obtaining medical care; f) stealing Social Security
22 and other government benefits; and g) applying for a driver's license, birth certificate or other
23 public document. Any of these activities can cause significant financial and emotional harm to a
24 victim. Even if the victim applies for and receives a replacement Social Security number, he or
25 she will not be free from risk.

26
27
28 ⁶ "Phishers Spoof CEO, Request W2 Forms," Krebsonsecurity.com. <http://bit.ly/25oAc2c>.

1 28. Plaintiff is an Employee whose 2016 Form W-2 data was disclosed by Sunrun.
2 Plaintiff provided confidential information to Sunrun including his name, date of birth and Social
3 Security number in connection with his employment. Plaintiff reasonably expected that Sunrun
4 would maintain the privacy of his confidential PII.

5 29. In addition, Plaintiff and class members are now and will be at risk of identity theft
6 for the rest of their lives, requiring constant diligence and monitoring. Upon information and
7 belief, other Employees have suffered harm as a result of the Data Breach in addition to
8 fraudulent tax returns and delays in receiving tax refunds.

9 **Sunrun's Inadequate Response to the Data Breach**

10 30. Sunrun has failed to provide adequate compensation for the Employees due to its
11 negligence. To date, Sunrun has offered Employees just two years of identity theft protection
12 through the Experian ProtectMyID service. Even if an Employee accepts the ProtectMyID
13 service, it will not provide Employees any compensation for the costs and burdens associated
14 with the fraudulent tax returns that were filed prior to an Employee signing up for ProtectMyID.
15 Sunrun has not offered Employees any assistance in dealing with the IRS or state tax agencies.
16 Nor has Sunrun offered to reimburse Employees for the costs – current and future – incurred as a
17 result of falsely filed tax returns.

18 31. The offered ProtectMyID service is inadequate to protect the Employees from the
19 threats they face. It does nothing to protect *against* identity theft. Instead, it only provides a
20 measure of assistance after identity theft has been discovered. For example, ProtectMyID only
21 monitors Employees' *credit reports* – but fraudulent activity, such as the filing of a false tax
22 return, may not appear on a credit report. ProtectMyID *does not* provide real time monitoring of
23 Employees' credit cards and bank account statements. Employees must pay extra for that service.
24 Although ProtectMyID offers up to \$1 million of identity theft insurance, the coverage afforded is
25 limited and often duplicative of (or inferior to) basic protections provided by banks and credit
26 card companies. Thus, providing adequate identity theft protection is an essential component of
27 the injunctive relief sought in this case.

32. Many websites that rank identity protection services are critical of ProtectMyID. NextAdvisor ranks ProtectMyID at the bottom of comparable services, noting that it “lacks in protection; only includes Experian credit report monitoring; 7-day trial for \$1 with enrollment; credit score and other credit reports cost extra.”⁷ BestIDtheftCompanies.com ranks ProtectMyID at No 30 with a score of just 4.4 out of 10 (and a “User Score” of just 1.3).⁸

Class Action Allegations

a. Plaintiff brings these claims pursuant to California Code of Civil Procedure § 382 on behalf of a class of similarly situated persons, which she proposes to be defined as follows: “All current and former Sunrun Inc. and Sunrun Installation Services, Inc. employees whose PII was compromised as a result of the Data Breach.”

b. Plaintiff also seeks to represent a sub-class defined as: “All current and former Sunrun Inc. and Sunrun Installation Services, Inc. employees who are citizens of California and whose PII was compromised as a result of the Data Breach.”

33. **Numerosity.** The proposed class and sub-class contain at least hundreds of individuals throughout California and the United States. Joinder of all class and sub-class members is impracticable. Class and sub-class members can be identified through Sunrun’s records.

34. **Commonality.** Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual class and sub-class members. Common questions include:

- a. Whether and to what extent Sunrun had a duty to protect the class and sub-class members’ PII;
- b. Whether Sunrun breached its duty to protect the class and sub-class members’ PII;
- c. Whether Sunrun disclosed class and sub-class members’ PII.

⁷ “Identity Theft Protection Reviews & Prices,” NextAdvisor.com. <http://bit.ly/1UCnsRP>.

⁸ “Experian ProtectMyID,” bestidtesftcompanies.com. <http://bit.ly/1Rh1YGy>.

- d. Whether Sunrun timely, accurately, and adequately informed class and sub-class members that their PII had been compromised;
- e. Whether class and sub-class members are entitled to damages; and
- f. Whether class and sub-class members are entitled to injunctive relief.

35. **Typicality.** Plaintiff's claims are typical of the claims of members of the proposed class and sub-class because, among other things, Plaintiff and class members sustained similar injuries as a result of Sunrun's uniform wrongful conduct; Sunrun owed the same duty to each class and sub-class member; and their legal claims arise from the same conduct by Sunrun.

36. **Adequacy.** Plaintiff will fairly and adequately protect the interests of the proposed classes. Plaintiff's interests do not conflict with the class members' interests. Plaintiff has retained class counsel experienced in class action litigation to prosecute this case on behalf of the classes.

37. **Superiority.** A class action is superior to other available means for the fair and efficient adjudication of this controversy. Individual joinder of all proposed class and sub-class members is not practicable, and questions of law and fact common to the class predominate over any questions affecting only individual members of the class. Each member of the class and sub-class has been damaged and is entitled to recovery by reason of Defendant's illegal policies and/or practices.

38. Class action treatment will allow those similarly-situated persons to litigate their claims in the manner that is most effective and economical for the parties and the judicial system. Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

39. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all proposed class and sub-class members is impractical. Even if every proposed class and sub-class member could afford individual litigation, the court system could not. It would be unduly burdensome to the courts if individual litigation of numerous cases were to be required. Individualized litigation also would present the potential for varying, inconsistent, or contradictory judgments and would

1 magnify the delay and expense to all parties and to the court system resulting from multiple trials
2 of the same complex factual issues. By contrast, the conduct of this action as a class action with
3 respect to some or all of the issues presented herein gives rise to fewer management difficulties,
4 conserves the resources of the court system and the parties and protects the rights of each
5 proposed class and sub-class member. Further, it prevents the very real harm that would be
6 suffered by numerous putative class members who simply will be unable to enforce individual
7 claims of this size on their own, and by Defendant's competitors, who will be placed at a
8 competitive disadvantage as their reward for obeying the law. Plaintiff does not anticipate
9 difficulties in the management of this action.

10 **CAUSES OF ACTION**

11 **I. FIRST CAUSE OF ACTION**

12 **(Negligence)**

13 40. Plaintiff realleges and incorporates by reference all prior allegations as if fully set
14 forth herein.

15 41. The Employees are or were employed by Defendants during the 2016 tax year and
16 were already or will be issued a 2016 Form W-2 from Defendants. As a condition of their
17 employment, the Employees were obligated to provide Defendants with certain PII, including
18 their names, addresses, and Social Security numbers.

19 42. Sunrun had full knowledge of the sensitivity of the PII and the types of harm that
20 Plaintiff and class members could and would suffer if the PII were wrongfully disclosed. Sunrun
21 had a duty to Plaintiff and each class and sub-class member to exercise reasonable care in
22 holding, safeguarding and protecting that information. Plaintiff and the class and sub-class
23 members were the foreseeable victims of any inadequate safety and security practices. Plaintiff
24 and the other class and sub-class members had no ability to protect their data that was in Sunrun's
25 possession.

26 43. Sunrun's duty to the Plaintiff and other class and sub-class members included,
27 *inter alia*, establishing processes and procedures to protect the PII from wrongful disclosure and
28 training employees who had access to the PII as to those processes and procedures. Sunrun is a

1 significant player in the insurance industry, and Sunrun, its officers, directors and management
2 are all well aware of the risks associated with the wrongful disclosure of PII and the threats to PII
3 posed by hackers, scammers, and other cybercriminals.

4 44. In addition, Sunrun had a duty to timely and adequately disclose to Plaintiff and
5 the other class and sub-class members that their PII had been compromised. Such timely
6 disclosure was necessary to allow Plaintiff and the other class members to (i) purchase identity
7 protection services; (ii) monitor their bank accounts, credit cards and other financial accounts;
8 and (iii) take other steps to protect against identity theft and the fraudulent use of their PII by
9 third parties.

10 45. Sunrun has already admitted that the PII of Plaintiff and other class and sub-class
11 members was wrongfully disclosed as a result of the Data Breach. Sunrun further admitted that
12 the Data Breach was the result of Sunrun's error.

13 46. As a result of Sunrun's negligence, Plaintiff and the class and sub-class members
14 have suffered and will continue to suffer damages and injury including, but not necessarily
15 limited to: a) out-of-pocket costs associated with addressing false tax returns filed with the IRS
16 and state tax agencies; b) increased future out of pocket costs in connection with preparing and
17 filing tax returns; c) out-of-pocket costs associated with procuring identity protection and
18 restoration services; d) in the event of future identity theft, out-of-pocket costs associated with
19 repairing credit, reversing fraudulent charges, and other harms; and e) lost productivity and
20 enjoyment as a result of time spent monitoring, addressing and correcting future consequences of
21 the Data Breach.

22 47. Sunrun breached its duty to Plaintiff and the class and sub-class members by
23 failing to maintain proper security measures, policies and procedures, and training. Sunrun failed
24 to timely notify Plaintiff and the class and sub-class members of the Data Breach. Plaintiff and
25 the class and sub-class members have been harmed as a direct and proximate result of Sunrun's
26 negligence. Plaintiff and the class and sub-class members will continue to be harmed as a direct
27 and proximate result of Sunrun's negligence.
28

1 48. Plaintiff and the class and sub-class members are entitled to money damages for all
2 out-of-pocket costs caused by Sunrun's negligence. Plaintiff also seeks reasonable attorneys' fees
3 and costs under the applicable law, including California Code of Civil Procedure § 1021.5.

4 **II. SECOND CAUSE OF ACTION**

5 **(Violation of Unfair Competition Law**

6 **California Business and Professional Code Section 17200, et seq.)**

7 49. Plaintiff realleges and incorporates by reference all prior allegations as if fully set
8 forth herein.

9 50. Sunrun engaged in unfair and unlawful business practices in violation of the
10 Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.* ("UCL"). Sunrun's acts,
11 omissions and conduct constitute unfair and unlawful business practices under the UCL.

12 51. Sunrun's practices were unlawful and in violation of Civil Code §1798.81.5
13 because Sunrun failed to take reasonable measures in protecting Plaintiff's and the class and sub-
14 class members' PII.

15 52. Sunrun's practices were also unlawful and in violation of Civil Code § 1798.82
16 because Sunrun's notice to Plaintiff and the class and sub-class members concerning the Data
17 Breach, as required by the statute, failed to fully disclose the extent of the Data Breach.

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

27 54. Sunrun had exclusive knowledge about the extent of the Data Breach, including
28 during the days following the Data Breach.

1 55. But for Sunrun's misrepresentations and omissions, Plaintiff and the class and sub-
2 class members would not have provided the PII that they provided to Sunrun or would have
3 insisted that their PII be more securely protected and removed from Sunrun's systems promptly
4 after their employment ended. They also would have taken additional steps to protect their
5 identities and to protect themselves from the sort of harm that could flow from Sunrun's lax
6 security measures. But for Sunrun's misrepresentations and omissions, Plaintiff and the class and
7 sub-class members would not be experiencing identity theft, identity fraud, and/or the increased
8 risk of harm they are now facing, as a result of the Data Breach. But for the fact that Sunrun sat
9 on information regarding the Data Breach, rather than immediately disclosing it, Plaintiff and the
10 and sub-class class members would have taken more immediate steps to protect their identities
11 and they would have been able to minimize the harm they have suffered as a result of the Data
12 Breach.

13 56. As a direct and proximate result of Sunrun's unlawful and unfair business
14 practices as alleged herein, Plaintiff and the class and sub-class members have suffered injury in
15 fact. Plaintiff and the classes have been injured in that their personal and financial PII has been
16 compromised, subject to identity theft, identity fraud, and/or is at risk for future identity theft and
17 fraudulent activity on their financial accounts. Class and sub-class members have also lost money
18 and property that would not have been lost but for Sunrun's unlawful and unfair conduct.

19 57. As a direct and proximate result of Sunrun's unlawful and unfair business
20 practices as alleged herein, Plaintiff and class and sub-class members already suffer from identity
21 theft, identity and financial fraud, and/or a continuing increased risk of identity theft and financial
22 and medical fraud due to the compromise, publication, and/or unauthorized use of their PII.
23 Plaintiff and the class and sub-class members have also been injured by, among other things: (1)
24 the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or
25 use of their PII entrusted to Sunrun for the purpose of deriving employment from Sunrun and
26 with the expectation that Sunrun would safeguard their PII against disclosure and not allow
27 access and misuse of their PII by others; (3) the compromise, publication, and/or theft of their PII;
28 (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft

1 and/or unauthorized use of financial and medical accounts; (5) lost opportunity costs associated
2 with effort expended and the loss of productivity from addressing and attempting to mitigate the
3 actual and future consequences of the breach, including but not limited to efforts spent
4 researching how to prevent, detect, contest and recover from identity and health care/medical data
5 misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit
6 misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit
7 reports and assets; (7) unauthorized use of compromised PII to open new financial and/or health
8 care or medical accounts; (8) tax fraud and/or other unauthorized charges to financial, health care
9 or medical accounts and associated lack of access to funds while proper information is confirmed
10 and corrected; (9) the continued risk to their PII, which remains in Sunrun's possession and are
11 subject to further breaches so long as Sunrun fails to undertake appropriate and adequate
12 measures to protect the PII in its possession; and (10) future costs in terms of time, effort and
13 money that will be expended to prevent, detect, contest, and repair the impact of the PII
14 compromised as a result of the Data Breach for the remainder of the Plaintiff's and the class and
15 sub-class members' lives.

16 58. As a result of Sunrun's violations of the UCL, Plaintiff and the class and sub-class
17 members are entitled to injunctive relief, including, but not limited to an order that Sunrun: (1)
18 engage third party security auditors/penetration testers as well as internal security personnel to
19 conduct testing consistent with prudent industry practices, including simulated attacks,
20 penetration tests, and audits on Sunrun's systems on a periodic basis; (2) engage third party
21 security auditors and internal personnel to run automated security monitoring consistent with
22 prudent industry practices; (3) audit, test, and train its security personnel regarding any new or
23 modified procedures; (4) purge, delete and destroy, in a secure manner, employee data not
24 necessary for its business operations; (5) conduct regular database scanning and security checks
25 consistent with prudent industry practices; (6) periodically conduct internal training and education
26 to inform internal security personnel how to identify and contain a breach when it occurs and
27 what to do in response to a breach consistent with prudent industry practices; (7) receive periodic
28 compliance audits by a third party regarding the security of the computer systems Sunrun uses to

1 store the PII of its current and former employees; (8) meaningfully educate its current and former
2 employees about the threats they face as a result of the loss of their PII to third parties, as well as
3 the steps they must take to protect themselves; and (9) provide ongoing identity theft protection,
4 monitoring, and recovery services to Plaintiff and class and sub-class members, as well as to their
5 dependents and designated beneficiaries of employment-related benefits through Sunrun.

6 59. Because of Sunrun's unlawful and unfair business practices, Plaintiff and the class
7 and sub-class members are entitled to relief, including attorneys' fees and costs, restitution,
8 declaratory and injunctive relief. Plaintiff also seeks reasonable attorneys' fees and costs under
9 applicable law including California Code of Civil Procedure § 1021.5.

10 **III. THIRD CAUSE OF ACTION**

11 **(Declaratory Judgment)**

12 60. Plaintiff realleges and incorporates by reference all prior allegations as if fully set
13 forth herein.

14 61. As set forth above, Plaintiff and the class and sub-class members have valid claims
15 against Sunrun for negligence and violations of the UCL. An actual controversy has arisen in the
16 wake of Sunrun's Data Breach regarding Sunrun's current obligations to provide reasonable data
17 security measures to protect the PII of Plaintiff and the class and sub-class members.

18 62. Plaintiff thus seeks a declaration that to comply with its existing obligations,
19 Sunrun must implement specific additional, prudent industry security practices, as outlined
20 below, to provide reasonable protection and security to the PII of Plaintiff and the class and sub-
21 class members. Specifically, Plaintiff and the class and sub-class members seek a declaration that
22 (a) Sunrun's existing security measures do not comply with its obligations, and (b) that to comply
23 with its obligations, Sunrun must implement and maintain reasonable security measures on behalf
24 of Plaintiff and the class and sub-class, including, but not limited to: (1) engaging third party
25 security auditors/penetration testers as well as internal security personnel to conduct testing
26 consistent with prudent industry practices, including simulated attacks, penetration tests, and
27 audits on Sunrun's systems on a periodic basis; (2) engaging third party security auditors and
28 internal personnel to run automated security monitoring consistent with prudent industry

1 practices; (3) auditing, testing, and training its security personnel regarding any new or modified
2 procedures; (4) purging, deleting and destroying, in a secure manner, employee data not
3 necessary for its business operations; (5) conducting regular database scanning and security
4 checks consistent with prudent industry practices; (6) periodically conducting internal training
5 and education to inform internal security personnel how to identify and contain a breach when it
6 occurs and what to do in response to a breach consistent with prudent industry practices; (7)
7 receiving periodic compliance audits by a third party regarding the security of the computer
8 systems Sunrun uses to store the personal information of its current and former employees; (8)
9 meaningfully educating its current and former employees about the threats they face as a result of
10 the loss of their PII to third parties, as well as the steps they must take to protect themselves; and
11 (9) providing ongoing identity theft protection, monitoring, and recovery services to Plaintiff and
12 class and sub-class members.

13 63. Plaintiff and each class and sub-class member is entitled to a declaration of rights
14 providing that Sunrun is obligated, pursuant to terms established by the Court, to reimburse said
15 individuals for any and all future harm caused by the Data Breach.

16 **IV. FOURTH CAUSE OF ACTION**

17 **(Breach of Implied Contract)**

18 64. Plaintiff realleges and incorporates by reference all prior allegations as if fully set
19 forth herein.

20 65. Sunrun Employees provided their PII in connection with their employment with
21 Sunrun in order to verify their identity, receive compensation and in order for Sunrun to have
22 complete employee records for tax purposes, amongst other things.

23 66. Plaintiff is an Employee class and sub-class member who provided various forms
24 of PII to Sunrun as a condition precedent to his employment with Sunrun, or in connection with
25 employer sponsored benefits.

26 67. Understanding the sensitive nature of PII, Sunrun implicitly promised Plaintiff and
27 the Employee class and sub-class members that it would take adequate measures to protect their
28 PII.

1 68. Indeed, a material term of this contract is a covenant by Sunrun that it will take
2 reasonable efforts to safeguard Employees' PII.

3 69. Sunrun's current and former employees, including Plaintiff and the Employee
4 class and sub-class members, relied upon this covenant and would not have disclosed their PII
5 without assurances that it would be properly safeguarded. Moreover, the covenant to adequately
6 safeguard the PII of Plaintiff and Employee class and sub-class members is an implied term, to
7 the extent it is not an express term.

8 70. Plaintiff and the Employee class and sub-class members fulfilled their obligations
9 under the contract by providing their PII to Sunrun.

10 71. Sunrun however, failed to safeguard and protect the PII of Plaintiff and the
11 Employee class and sub-class members. Sunrun's breach of its obligations under the contract
12 between the parties directly caused Plaintiff and Employee class and sub-class members to suffer
13 injuries.

14 72. Plaintiff, on behalf of himself and the Employee class and sub-class members,
15 respectfully request this Court award all relevant damages for Sunrun's breach of contract.

16 **PRAYER FOR RELIEF**

17 Plaintiff, on behalf of himself and on behalf of the proposed Employee class and sub-
18 class, requests that the Court:

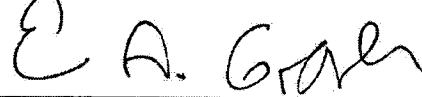
- 19 a. Certify this case as a class action, appoint Plaintiff as class representative and
20 appoint Plaintiff's counsel to represent the class;
21 b. Find that Sunrun breached its duty to safeguard and protect Plaintiff's and the class
22 and sub-class members' PII which was compromised in the Data Breach;
23 c. Award Plaintiff and class and sub-class members appropriate relief, including
24 actual damages, punitive damages, and statutory damages;
25 d. Award equitable, injunctive, declaratory relief as appropriate;
26 e. Award all costs, including experts' fees and attorneys' fees, and the costs of
27 prosecuting this action;
28

- 1 f. Award pre-judgment and post-judgment interest as prescribed by law; and
2 g. Grant additional legal or equitable relief as the Court may find just and proper.
3

4 Dated: February 9, 2017

Respectfully submitted,

5 **KELLER GROVER LLP**

6 

7 Eric A. Grover
8 Robert W. Spencer
9 Counsel for Plaintiff

10
11
12
13 **DEMAND FOR JURY TRIAL**

14 Plaintiff hereby demands a trial by jury on all issues so triable.
15

16 Dated: February 9, 2017

Respectfully submitted,

17 **KELLER GROVER LLP**

18 

19 Eric A. Grover
20 Robert W. Spencer
21 Counsel for Plaintiff
22
23
24
25
26
27
28