Tina Wolfson (SBN 174806)
twolfson@ahdootwolfson.com
Theodore W. Maya (SBN 223242)
tmaya@ahdootwolfson.com
Deborah De Villa (SBN 312564)
ddevilla@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, California 91505
Tel. (310) 474.9111
Fax: (310) 474.8585

Counsel to Plaintiffs and the Proposed Class

[Additional counsel appear on signature page]

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

AVIVA KIRSTEN, and JEREMY PITTMAN, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

CALIFORNIA PIZZA KITCHEN, INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Aviva Kirsten and Jeremy Pittman, individually and on behalf of all others similarly situated, by and through their attorneys, Keller Lenkner LLC; Finkelstein, Blankinship, Frei-Pearson & Garber, LLP; and Ahdoot & Wolfson, PC, and for their class action complaint against Defendant California Pizza Kitchen, Inc., respectfully allege, upon their own knowledge or, where they lack personal knowledge, upon information and belief including the investigation of their counsel, as follows:

INTRODUCTION

1. Plaintiffs Aviva Kirsten ("Plaintiff Kirsten" or "Ms. Kirsten") and Jeremy Pittman ("Plaintiff Pittman" or "Mr. Pittman"; collectively, with Plaintiff Kirsten, "Plaintiffs") bring this class action lawsuit on behalf of themselves and all others similarly situated against Defendant California Pizza Kitchen, Inc. ("Defendant" or "CPK") as a result of Defendant's failure to safeguard and protect Plaintiffs' and the other Class Members' confidential information—including but not limited to Social Security numbers ("SSN"), dates of birth, financial information, and sensitive personally identifiable information that can be used to perpetrate identity theft (the "PII")—in Defendant's custody, control, and care.

2. Plaintiffs Kirsten and Pittman are both former employees of CPK. As a condition of their employment, each Plaintiff was required to and did supply CPK with their PII.

3. Unbeknown to Plaintiffs, Defendant did not have sufficient cyber-security procedures and policies in place to safeguard Plaintiffs' and Class Members' PII. As a result of this inadequate security, cybercriminals were able to gain access to Defendant's computer systems and records, including the PII of over 100,000 current and former CPK employees (the "Data Breach"). Plaintiffs and Class Members have suffered damages as a result of the unauthorized and preventable disclosure of their PII.

4. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity protections and protocols that were necessary to

protect the PII of current and former employees entrusted into Defendant's custody and care.

5. This lawsuit seeks redress for Defendant's unlawful disclosure of Plaintiffs' and Class Members' PII.

6. Plaintiffs assert causes of action for negligence, breach of fiduciary duty, breach of contract, and violations of California and other states' laws, all arising from Defendant's failure to safeguard Plaintiffs' and Class Members' PII. Plaintiffs bring claims for consequential damages, injunctive relief, and punitive damages.

PARTIES

7. Plaintiff Aviva Kirsten is and was a resident of Monterey County, California, who was an employee of CPK from approximately July 2021 to approximately September 2021, and whose PII was compromised in the Data Breach, as belatedly disclosed to her by CPK in a notice she received in approximately November 2021.

8. Plaintiff Jeremy Pittman is and was a resident of Los Angeles County, California, who was an employee of CPK from approximately June 2021 to approximately August 2021, and whose PII was compromised in the Data Breach, as belatedly disclosed to him by CPK in a notice he received in approximately November 2021.

9. Defendant California Pizza Kitchen, Inc. is a corporation organized under the laws of the state of Delaware and with a principal place of business at 575 Anton Boulevard, Suite 100, in Costa Mesa, California. At all times material hereto, Defendant acted by and through agents, employees, and representatives, who were acting in the course and scope of their respective agency or employment and/or in the promotion of CPK's business, mission, and/or affairs.

JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2) because the amount in controversy

exceeds $5,000,000.00, excluding interest and costs, and at least one member of the proposed Class is a citizen of a state different from Defendant.

11. This Court has personal jurisdiction over Defendant because Defendant regularly conducts business in the state of California and is headquartered in Orange County, California.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District, Defendant caused harm to Plaintiffs and Class Members through its actions in this District, and Defendant's principal place of business is located within this District.

FACTUAL ALLEGATIONS

OVERVIEW OF CALIFORNIA PIZZA KITCHEN

13. CPK is an American casual dining restaurant chain that operates over 250 casual dining restaurants in 32 states and internationally, with approximately 14,000 employees.

14. In the regular course of its business and employment practices, CPK collects and maintains the PII of employees and former employees. CPK requires prospective and current employees to provide PII—including highly sensitive SSNs—as part of the employment and hiring process, and as a condition for employment.

15. Plaintiffs and Class Members are, or were, employees of CPK who entrusted their PII to CPK.

THE CPK DATA BREACH AND SUBSEQUENT NOTICE

16. In or about September 2021, CPK discovered that an unauthorized individual, or unauthorized individuals, gained access to CPK's network systems. UIA has not revealed how long cybercriminals may have had access to its network.

17. In a Notice of Data Breach, CPK disclosed that "[o]n or about September 15, 2021, CPK learned of a disruption to certain systems on our computing environment."[1] The Notice identified that "[o]n October 4, 2021, the investigation confirmed that certain files on [CPK's] systems had been subject to unauthorized access."[2]

18. According to the Maine Attorney General's website, the breach was an "external system breach" that affected 103,767 people.[3]

CPK KNEW OF THE RISKS OF DATA BREACHES AND COMPROMISED SENSITIVE INFORMATION

19. CPK had obligations created by contract, industry standards, common law, and representations made to current and former employees to keep Plaintiffs' and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

20. Defendant's data security obligations are and were particularly important given the substantial increase in cyberattacks and/or data breaches widely reported on in the last few years. In fact, in the wake of this rise in data breaches, the Federal Trade Commission ("FTC") has issued an abundance of guidance for companies and institutions that maintain individuals' PII.[4]

---

[1] *See* Letter from James F. Hyatt II, CEO/President, California Pizza Kitchen (Nov. 15, 2021), https://oag.ca.gov/system/files/California%20Pizza%20Kitchen%20-%20Sample%20Notice.pdf.

[2] *Id.*

[3] OFFICE OF THE MAINE ATTORNEY GENERAL, *Data Breach Notifications,* https://apps.web.maine.gov/online/aeviewer/ME/40/ea812f00-c605-4b8e-a6e2-9dd53169b256.shtml (last visited Dec. 9, 2021).

[4] *See, e.g.,* FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS (2016), https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

21. Indeed, according to a report by Risk Based Security, Inc., by the end of June 2020 was already the "worst year on record" in terms of records exposed in data breaches.[5]

22. Therefore, Defendant clearly knew or should have known of the risks of data breaches and thus should have ensure that adequate protections to safeguard employees' PII were in place.

23. Plaintiffs and Class Members were obligated to provide Defendant with their PII as part of their employment relationships with Defendant.

24. Due to inadequate security against unauthorized intrusions, cybercriminals breached Defendant's computer systems on or about September 15, 2021. Data breaches were a known threat to CPK, and the Data Breach resulted in the criminals unlawfully obtaining access to employees' PII, including their identities and SSNs.

DATA BREACHES LEAD TO IDENTITY THEFT

25. Data breaches are more than just technical violations of their victims' rights. By accessing a victim's personal information, the cybercriminal can ransack the victim's life: withdraw funds from bank accounts, get new credit cards or loans in the victims' name, lock the victim out of his or her financial or social media accounts, send out fraudulent communications masquerading as the victim, file false tax returns, destroy their credit rating, and more.

26. As the United States Government Accountability Office noted in a June 2007 report on data breaches ("GAO Report"), identity thieves use identifying data such as SSNs to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[6] As the GAO Report states, this type of identity theft is more harmful than

---

[5] *See* RISKBASED SECURITY 2020 Q3 REPORT DATA BREACH QUICKVIEW (2020), https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Q3%20Data%20Breach%20QuickView%20Report.pdf.

[6] *See* UNITED STATES GOV'T ACCOUNTABILITY OFFICE, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN (June 2007), https://www.gao.gov/new.items/d07737.pdf.

any other because it often takes time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

27. In addition, the GAO Report states that victims of this type of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[7]

28. Identity theft victims are frequently required to spend many hours and large sums of money repairing the adverse impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

29. There may be a time lag between when sensitive information is stolen and when it is used. According to the GAO Report:

> "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[8]

30. With access to an individual's PII, cyber criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[9]

---

[7] *Id.* at 2, 9.

[8] *Id*. at 29 (emphasis added).

[9] *See* FED. TRADE COMM'N, *Warning Signs of Identity Theft*, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited Dec. 9, 2021).

31. Such personal information is such a crucial commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, SSNs, and other sensitive information directly on various internet websites making the information publicly available.

32. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[10]

33. Theft of SSNs also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

34. Due to the highly sensitive nature of SSNs, theft of SSNs in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[11]

35. It is within this context that Plaintiffs and all other Class Members must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black-market.

---

[10] IDENTITY THEFT RESOURCE CENTER, 2021 CONSUMER AFTERMATH REPORT (May 2021), file:///Users/windyloritsch/Downloads/ITRC_2021_Consumer_Aftermath_Report.pdf

[11] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019, 3:39 PM EDT), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

DEFENDANT DELAYED NOTICE TO PLAINTIFFS AND CLASS MEMBERS

36. Despite becoming aware of the Data Breach on or about September 15, 2021, and receiving confirmation that employees' PII had been exposed by no later than October 4, 2021, Defendant only notified Plaintiffs and other impacted Data Breach victims that its systems had been breached and that their PII was compromised on or about November 15, 2021—two months after Defendant learned of the Data Breach.

37. There was no justifiable reason for CPK to delay providing notice for so long, and CPK has even represented that providing notice to affected Class Members "has not been delayed by law enforcement."[12]

38. On or about November 15, 2021, Defendant sent letters to Plaintiffs and other Class Members advising them that their PII had been subject to unauthorized access and had been compromised on or about September 15, 2021 (the "Letter Notification"). The Letter Notification offered only a single year of credit monitoring through Experian IdentityWorks, and only for individuals who signed up for such monitoring by January 31, 2022.

DEFENDANT FAILED TO ADHERE TO DATA PRIVACY OBLIGATIONS

39. In the ordinary course of, and as a condition of, their employment with CPK, Plaintiffs, like tens of thousands of other employees, provided PII, including but not limited to, their SSNs, to Defendant.

40. CPK maintains this PII within its computer systems and data infrastructure.

41. Furthermore, Plaintiffs and Class Members all entered into written agreements with Defendant as part of, and as a precondition to, their employment with CPK. The employment agreements involved a mutual exchange of consideration whereby Plaintiffs agreed to perform particular job duties and responsibilities in the furtherance of

[12] Carly Page, *California Pizza Kitchen spills over 100,000 employee Social Security numbers*, TECHCRUNCH (NOV. 18, 2021, 7:59 AM PST), https://techcrunch.com/2021/11/18/california-pizza-kitchen-data-breach/.

CPK's business, in exchange for CPK's promise of employment with wages, benefits, and secure PII. These agreements contained or incorporated representations that Defendant would protect Class Members' PII.

42. By failing to adequately protect Plaintiffs' and Class Members' PII, Defendant violated its legal obligations and its contractual obligations.

43. Defendant compounded the actual and potential harm arising from the Data Breach by not notifying Plaintiffs and other Class Members of the compromise of their PII until November 2021. Defendant suggested in the Letter Notification that Plaintiffs and Class Members review account statements, monitor credit reports, and perhaps institute security freezes on their financial accounts to safeguard their financial well-being from harm arising from the Data Breach. Putting aside that this shifts the onus of dealing with the fallout of the Data Breach on Defendant's unjustified delay in notifying Plaintiffs and the Class that they were victims of the Data Breach will dilute any salutary effect that might come from these suggestions.

44. Defendant's security failure demonstrates that it failed to honor its duties and promises by not:

a. Maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Adequately protecting Plaintiffs' and the Class Members' PII;

c. Properly monitoring its own data security systems for existing intrusions; and

d. Ensuring that agents, employees, and others with access to PII employed reasonable security procedures.

45. Plaintiffs and all Class Members have consequently suffered harm by virtue of the compromise and exposure of their PII—including, but not limited to, (i) an imminent risk of future identity theft; (ii) lost time and money expended to mitigate the threat of identity theft; (iii) diminished value of personal information; and (iv) a loss of privacy. Plaintiffs and Class Members were also injured because they did not receive the full value

of the employment for which they bargained; to wit, a wage plus adequate data security. Plaintiffs and all members of the proposed Class are and will continue to be at imminent risk for tax fraud and identify theft and the attendant dangers thereof for the rest of their lives because their PII, including SSNs, is in the hands of cybercriminals.

DEFENDANT'S INADEQUATE RESPONSE TO THE DATA BREACH

46. Defendant's Letter Notification stated that it is "reviewing existing security policies and have implemented additional measures to further protect against similar incidents."[13] No details were provided, and thus it cannot be determined from the Letter Notification whether Defendant did any of the foregoing, or if it did, whether these enhancements are sufficient to prevent recurrences similar to the Data Breach.

47. The belated Letter Notification also included an offer from Defendant of one year of free credit monitoring and identity theft resolution services through a third-party provider, Experian. Defendant, however, offered an unreasonably short window of opportunity to claim these services, with victims of the Data Breach needing to claim these services by January 31, 2022, or be closed out. In addition, one year of credit monitoring services is insufficient, given that Plaintiffs' and the Class Members' risk of identity theft will continue throughout their lives.

48. Absent from the Letter Notification is any offer of compensation for out-of-pocket losses which the Class has and foreseeably will sustain—including, but not limited to, time spent to rectify any and all harms that resulted from the Data Breach. Plaintiffs and Class Members have suffered financial loss, including but not limited to lost opportunity costs for the time and effort necessary to remedy the harm they suffered. Thus, Defendant's offer in the Letter Notification fails to make Plaintiffs and the other members of the Class whole.

---

[13] https://apps.web.maine.gov/online/aeviewer/ME/40/ea812f00-c605-4b8e-a6e2-9dd53169b256/83c0fbf0-f0e4-40ef-b34e-127f3754a13e/document.html (last visited Dec. 9, 2021)

CLASS ALLEGATIONS

49. Plaintiffs propose the following class definition(s), subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiffs bring this action and seek certification of the following Classes:

> **National Class:** All persons whose PII was exposed in the Data Breach, including all persons who were sent a notice of the Data Breach. (the "National Class" or the "Class").
>
> **California Sub-Class:** All persons in California whose PII was exposed in the Data Breach, including all persons in California who were sent a notice of the Data Breach (the "California Sub-Class").
>
> **Multi-State Sub-Class:** All persons in Alaska, Arkansas, California, Colorado, Connecticut, Delaware, Washington D.C., Florida, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maryland, Massachusetts, Michigan, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, North Carolina, North Dakota, Oklahoma, Oregon, Rhode Island, South Carolina, Tennessee, Texas, Utah, Virginia, Washington, Wisconsin, or Wyoming whose PII was exposed in the Data Breach, including all persons in the aforementioned states who were sent a notice of the Data Breach (the "Multi-State Sub-Class"; together with the National Class and California Sub-Class, the "Classes").

50. Plaintiffs reserve the right to amend the above definitions, or to propose other or additional classes, in subsequent pleadings and/or motions for class certification.

51. Plaintiffs are each a member of the Classes.

52. Excluded from the Classes are: (i) Defendant; any entity in which Defendant has a controlling interest; the officers, and directors of Defendant; and the legal representatives, heirs, successors, and assigns of Defendant; (ii) any judge assigned to hear this case (or any spouse or family member of any assigned judge); (iii) any juror selected to hear this case; and (iv) any and all legal representatives (and their employees) of the parties.

53. This action seeks both injunctive relief and damages.

54. Plaintiffs and the Classes satisfy the requirements for class certification for the following reasons:

55. **Numerosity.** According to CPK's notice to the Attorney General of the State of Maine concerning the Data Breach, the Data Breach affected approximately 103,767 individuals.[14] Therefore, the members of the Class are so numerous that their individual joinder is impracticable. The precise number of persons in the Class and their identities and addresses may be ascertained or corroborated from Defendant's records. If deemed necessary by the Court, members of the Class may be notified of the pendency of this action.

56. **Common Questions of Law and Fact.** There are questions of law and fact common to the Class that predominate over any questions affecting only individual members, including:

a. Whether and to what extent Defendant had a duty to protect Plaintiffs' and Class Members' PII.

b. Whether Defendant breached its duty to protect Plaintiffs' and Class Members' PII.

c. Whether Defendant's data security systems prior to the Data Breach met the requirements of relevant laws;

d. Whether Defendant's data security systems prior to the Data Breach met industry standards;

e. Whether Plaintiffs' and other Class Members' PII was compromised in the Data Breach;

f. Whether the actions and or/inaction of Defendant caused Plaintiffs' and Class Members' PII to be disclosed or compromised;

g. Whether Defendant was negligent; and

[14] OFFICE OF THE MAINE ATTORNEY GENERAL, *Data Breach Notifications,* https://apps.web.maine.gov/online/aeviewer/ME/40/ea812f00-c605-4b8e-a6e2-9dd53169b256.shtml (last visited Dec. 9, 2021).

h. Whether Plaintiffs and other Class Members are entitled to damages as a result of Defendant's conduct.

57. **Typicality.** The claims or defenses of Plaintiffs are typical of the claims or defenses of the proposed Class because Plaintiffs' claims are based upon the same legal theories and same violations of law. Plaintiffs' grievances, like the proposed Class Members' grievances, all arise out of the same business practices and course of conduct by Defendant.

58. **Adequacy.** Plaintiffs will fairly and adequately represent the Class on whose behalf this action is prosecuted. Their interests do not conflict with the interests of the Class.

59. Plaintiffs and their chosen attorneys—Finkelstein, Blankinship, Frei-Pearson & Garber, LLP ("FBFG"), Keller Lenkner, LLC ("Keller Lenkner"), and Ahdoot & Wolfson, PC ("AW")—are familiar with the subject matter of the lawsuit and have full knowledge of the allegations contained in this Complaint.

60. FBFG has been appointed as lead counsel in several complex class actions across the country and has secured numerous favorable judgments in favor of its clients, including in cases involving data breaches. FBFG's attorneys are competent in the relevant areas of the law and have sufficient experience to vigorously represent the Class Members. Finally, FBFG possesses the financial resources necessary to ensure that the litigation will not be hampered by a lack of financial capacity and is willing to absorb the costs of the litigation.

61. Keller Lenkner is the 2021 Trial Strategy Innovation Law Firm of the Year, as named by The National Law Journal and American Lawyer Media. Keller Lenkner is a national firm that has secured recovery on behalf of hundreds of thousands of plaintiffs across America and is dedicated to zealously representing members of the Class. Keller Lenkner has the financial resources and staffing necessary to support the costs of this litigation.

62. AW is among the most experienced data privacy class action firms in the United States, having represented plaintiffs in nationwide class actions and other complex, large-scale litigations for nearly three decades. AW routinely is appointed to leadership positions in some of the most prominent data breach and data privacy litigations in the country. AW possesses and is willing to expend the resources to prosecute this action efficiently and in the best interests of the Class Members

63. **Superiority.** A class action is superior to any other available method for adjudicating this controversy. The proposed class action is the surest way to fairly and expeditiously compensate such a large a number of injured persons, to keep the courts from becoming paralyzed by hundreds—if not thousands—of repetitive cases, and to reduce transaction costs so that the injured Class Members can obtain the most compensation possible.

64. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which in any event might cause inconsistent results.

b. When the liability of Defendant has been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendant to all Class Members, in terms of money damages due and in terms of equitable relief, can be determined in this single proceeding rather than in multiple, individual proceedings where there will be a risk of inconsistent and varying results.

c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class Members are forced to bring individual suits, the transactional costs, including those incurred by Defendant, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with the identical fact patterns and

the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class Members and as to Defendant.

d. This lawsuit presents no difficulties that would impede its management by the Court as a class action. Class certification issues can be easily determined because the Class includes only CPK employees and former employees, the legal and factual issues are narrow and easily defined, and the Class membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class Members can be identified from Defendant's records, such that direct notice to the Class Members would be appropriate.

65. In addition, Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive or equitable relief with respect to the Class.

FIRST CAUSE OF ACTION

NEGLIGENCE
(On Behalf Of Plaintiffs And All Class Members)

66. Plaintiffs repeat each and every allegation of this Complaint as if fully set forth at length herein.

67. Defendant required Plaintiffs and the Class Members to submit non-public personal information to Defendant in order to obtain employment with CPK.

68. Defendant owed a duty to Plaintiffs and to the Class to exercise reasonable care in obtaining, securing, safeguarding, properly disposing of and protecting Plaintiffs' and Class Members' PII within its control from being compromised by or being accessed by unauthorized third parties. This duty included, among other things, maintaining adequate control over its computer systems and network so as to prevent unauthorized access thereof.

69. Defendant owed a duty of care to the Plaintiffs and members of the Class to provide security, consistent with industry standards, to ensure that its computer systems adequately protected the PII of the individuals who entrusted it to the Defendant.

70. Defendant alone was in a position to ensure that its systems were sufficient to protect against the harm to Plaintiffs and the members of the Class from the Data Breach.

71. In addition, Defendant had a duty to use reasonable security measures under Section A of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

72. Defendant's duty to use reasonable care in protecting the PII arose not only as a result of the common law and the statutes and regulations described above, but also because it is bound by, and has committed to comply with, industry standards for the protection of confidential information.

73. Defendant breached its common law, statutory, and other duties—and thus, was negligent—by failing to use reasonable measures to protect employees' PII, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs' and the Class Members' PII;

b. failing to adequately monitor the security of its networks and systems;

c. allowing unauthorized access to Plaintiffs' and the Class Members' PII; and

d. failing to warn Plaintiffs and other Class Members about the Data Breach in a timely manner so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

74. Defendant owed a duty of care to the Plaintiffs and the members of the Class because they were foreseeable and probable victims of any inadequate security practices.

75. It was foreseeable that Defendant's failure to use reasonable measures to protect PII and to provide timely notice of the Data Breach would result in injury to Plaintiffs and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiffs and the members of the Class were reasonably foreseeable.

76. It was therefore foreseeable that the failure to adequately safeguard PII would result in one or more of the following injuries to Plaintiffs and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

77. Defendant knew or reasonably should have known of the inherent risks in collecting and storing the PII of Plaintiffs and members of the Class and the critical importance of providing adequate security of that information, yet despite the foregoing had inadequate cyber-security systems and protocols in place to secure the PII.

78. As a result of the foregoing, the Defendant unlawfully breached its duty to use reasonable care to protect and secure the PII of Plaintiffs and the Class which Plaintiffs and members of the Class were required to provide to Defendant as a condition of employment with CPK.

79. Plaintiffs and members of the Class reasonably relied on the Defendant to safeguard their information, and while Defendant was in a position to protect against the harm from a data breach, Defendant negligently and carelessly squandered that opportunity. As a proximate result, Plaintiffs and members of the Class suffered and continue to suffer the consequences of the Data Breach.

80. Defendant's negligence was the proximate cause of harm to Plaintiffs and members of the Class.

81. Had Defendant not failed to implement and maintain adequate security measures to protect the PII of its employees, the Plaintiffs' and Class Members' PII would

not have been exposed to unauthorized access and stolen, and they would not have suffered any harm.

82. However, as a direct and proximate result of Defendant's negligence, Plaintiffs and members of the Class have been seriously and permanently damaged by the Data Breach. Specifically, Plaintiffs and members of the Class have been injured by, among other things; (1) the loss of the opportunity to control how their PII is used; (2) diminution of value and the use of their PII; (3) compromise, publication and/or theft of the Plaintiffs' and the Class Members' PII; (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 their efforts expended and the loss of productivity from addressing as well as attempting to mitigate the actual and future consequences of the breach including, but not limited to, efforts spent researching how to prevent, detect, and recover from identity 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 cost of the use, the use of credit, credit scores, credit reports, and assets; (7) unauthorized use of compromised PII to open new financial and/or healthcare and/or medical accounts; (8) tax fraud and/or other unauthorized charges to financial, healthcare or medical accounts and associated lack of access to funds while proper information is confirmed and corrected and/or imminent risk of the foregoing; (9) continued risks to their PII, which remains in the Defendant's possession and may be subject to further breaches so long as Defendant 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 spent trying to prevent, detect, contest and repair the effects of the PII compromised as a result of the Data Breach as a remainder of the Plaintiffs' and Class Members' lives.

83. Plaintiffs and the Class seek damages, injunctive relief, and other and further relief as the Court may deem just and proper.

SECOND CAUSE OF ACTION

NEGLIGENCE PER SE
(On Behalf Of Plaintiffs And All Class Members)

84. Plaintiffs repeat each and every allegation of this Complaint as if fully set forth at length herein.

85. Defendant's duties arise from, *inter alia*, Section 5 of the FTCA, 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as CPK, of failing to employ reasonable measures to protect and secure PII.

86. Defendant violated Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiffs' and other Class Members' PII and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable consequences of a data breach involving PII including, specifically, the substantial damages that would result to Plaintiffs and the other Class Members.

87. Defendant's violation of Section 5 of the FTCA constitutes negligence per se.

88. Plaintiffs and Class Members are within the class of persons that 5 of the FTCA was intended to protect.

89. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiffs and other Class Members as a result of the Data Breach.

90. It was reasonably foreseeable to Defendant that its failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit

appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiffs' and Class Members' PII to unauthorized individuals.

91. The injury and harm that Plaintiffs and the other Class Members suffered was the direct and proximate result of Defendant's violations of Section 5 of the FTCA. Plaintiffs and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*: (i) a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; and/or (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of medical identity theft they face and will continue to face.

THIRD CAUSE OF ACTION

INVASION OF PRIVACY BY INTRUSION
(On Behalf Of Plaintiffs And All Class Members)

92. Plaintiffs repeat each and every allegation of this Complaint as if fully set forth at length herein.

93. The Restatement (Second) of Torts states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977).

94. Plaintiffs and the Class Members had a reasonable expectation of privacy in the PII Defendant mishandled.

95. By intentionally failing to keep Plaintiffs' and the Class Members' PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties

for unauthorized use, Defendant intentionally invaded Plaintiffs' and Class Members' privacy by intrusion.

96. Defendant knew that ordinary persons in Plaintiffs' or the Class Members' positions would consider this an invasion of privacy and Defendant's intentional actions highly offensive and objectionable.

97. Defendant invaded Plaintiffs' and the Class Members' right to privacy and intruded into Plaintiffs' and the Class Members' private affairs by intentionally misusing and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

98. Defendant intentionally concealed from Plaintiffs and the Class Members an incident that misused and/or disclosed their PII without their informed, voluntary, affirmative, and clear consent.

99. In failing to protect Plaintiffs' and the Class Members' PII, and in intentionally misusing and/or disclosing their PII, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiffs' and the Class Members' rights to have such information kept confidential and private.

100. Plaintiffs and the Class Members sustained damages (as outlined above) as a direct and proximate consequence of the invasion of their privacy by intrusion, and therefore seek an award of damages.

FOURTH CAUSE OF ACTION

BREACH OF IMPLIED CONTRACT
(On Behalf Of Plaintiffs And All Class Members)

101. Plaintiffs repeat each and every allegation of this Complaint as if fully set forth at length herein.

102. Plaintiffs and members of the Class provided PII to the Defendant in connection with their obtaining employment from Defendant and were required to provide their PII as a condition of receiving employment.

103. Defendant would not have employed Plaintiffs, nor any members of the Class had Plaintiffs and members of the Class not provided various forms of PII to Defendant, including their SSNs and other privileged and confidential pieces of information.

104. Plaintiffs and members of the Class had no alternative and did not have any bargaining power with regard to providing their PII. The Defendant required disclosure of their PII as a condition to providing employment, which the Plaintiffs and members of the Class did.

105. When Plaintiffs and Class Members provided labor and their PII to Defendant in exchange for wages and other employment benefits, they entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such PII and to timely and accurately notify them if their data had been breached and compromised.

106. Defendant solicited and invited employees and employment candidates to provide their PII as part of its regular business practices. These individuals accepted Defendant's offers and provided their PII to Defendant. In entering into such implied contracts, Plaintiffs and the Class reasonably assumed that Defendant's data security practices and policies were reasonable and consistent with industry standards, and that Defendant would use part of the funds received from Plaintiffs and the Class to pay for adequate and reasonable data security practices.

107. Plaintiffs and the Class would not have provided and entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep the information secure.

108. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

109. Defendant breached its implied contracts with Plaintiffs and the Class by failing to safeguard and protect their PII and by failing to provide timely and accurate notice that their personal information was compromised as a result of the Data Breach.

110. As a direct and proximate result of Defendant's breaches of their implied contracts, Plaintiffs and the Class sustained actual losses and damages as described herein.

111. Plaintiffs and the Class seek damages, injunctive relief, and other and further relief as the Court may deem just and proper.

FIFTH CAUSE OF ACTION

VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW CAL. BUS. & PROF. CODE §§ 17200, *ET SEQ.* (On Behalf Of Plaintiffs And All Class Members)

112. Plaintiffs repeat each and every allegation of this Complaint as if fully set forth at length herein.

113. Defendant CPK is a "person" as that term is defined by, *inter alia*, Cal. Bus. & Prof. Code § 17201.

114. Defendant violated the California Unfair Competition Law ("UCL"), §§ 17200, *et seq*., by engaging in unlawful, unfair, and deceptive business acts and practices in relation to its failure to adequately secure its employees' PII.

115. Defendant's unlawful, unfair, and deceptive acts and practices include:

a. Defendant failed to implement and maintain reasonable data security policies, practices, and measures to protect the PII of Plaintiffs and Class Members from unauthorized access, disclosure, release, and theft, which was a direct and proximate cause of the Data Breach.

b. Defendant failed to:

i. Secure its internal company website;

ii. Secure access to its computer systems and servers;

iii. Comply with relevant industry standards for data and network security practices;

iv. Adequately secure or segment its company network(s);

v. Implement adequate system and event monitoring over its computer systems;

vi. Timely update and patch relevant programs related to its computer systems; and

vii. Implement the systems, policies, and procedures necessary to prevent a foreseeable security intrusion such as the Data Breach.

c. Defendant failed to identify and take adequate precautions against foreseeable security risks or to adequately improve its data security.

d. Defendant's lackluster security provides little, if any utility, and is particularly unfair within the meaning of the UCL when weighed against the resultant harm to Plaintiffs and the Class Members.

e. Defendant's lackluster security is also contrary to legislatively declared public policy that seeks to protect consumer data and ensure that entities that are trusted with it use appropriate security measures, as reflected in laws, including, *inter alia*, the FTCA, 15 U.S.C. § 45, California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5, 1798.82, and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 *et seq*.

f. Defendant's failure to implement and maintain reasonable computer security policies, procedures, and measures also lead to substantial injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition as contemplated under the UCL. Because Plaintiffs and the Class Members did not and could not know of CPK's inadequate security and compromise of their PII, they could not have reasonably avoided the harms caused by Defendant's lackluster security.

g. Defendant misrepresented that it would protect the privacy and confidentiality of Plaintiffs' and Class Members' PII, yet failed to do so. Defendant further omitted, suppressed, and/or concealed the material fact that it did not reasonably or adequately secure Plaintiffs' and the Class Members' PII.

h. Defendant misrepresented that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and

Class Members' PII, including all such duties as imposed by the FTCA, 15 U.S.C § 45; California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*.; and California's Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 *et seq*., yet failed to do so. Defendant further omitted, suppressed, and/or concealed the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' PII, including the duties imposed by the aforementioned statutes.

i. Defendant engaged in unlawful business practices by violating Cal. Civ. Code § 1798.82.

116. Defendant's misrepresentations and omissions to Plaintiffs and the Class Members were material because they were likely to deceive reasonable individuals about the adequacy of Defendant's data security and ability to protect the privacy of their PII.

117. Defendant intended to mislead Plaintiffs and members of the Class and induce them to rely on its misrepresentations and omissions.

118. If Defendant had disclosed to Plaintiffs and members of the Class that CPK's computer and data systems were not secure and, thus, vulnerable to cyberattack, CPK would have been unable to continue in business with such inadequate security policies, practices, and measures, and it would have been forced to adopt reasonable cybersecurity measures, in compliance with the law. However, Defendant instead received, maintained, and compiled Plaintiffs' and the Class Members' PII as part of the employment process without advising Plaintiffs California Sub-Class Members that CPK's data security practices were insufficient to maintain the safety and confidentiality of their PII. Accordingly, Plaintiffs and Class Members acted reasonably in relying on Defendant's misrepresentations and omissions, the veracity of which they could not have discovered prior to the Data Breach and Letter Notification.

119. Defendant acted intentionally, knowingly, and maliciously to violate the UCL in reckless disregard of Plaintiffs' and Class Members' rights.

120. As a direct and proximate result of Defendant's violations of the UCL, Plaintiffs and the Class sustained actual losses and damages as described herein.

121. Plaintiffs and the Class seek damages, injunctive relief, and other and further relief as the Court may deem just and proper.

122. Plaintiffs bring this Cause of Action on behalf of all Class Members pursuant to UCL § 17203, which authorized extraterritorial application of the UCL. In the alternative, Plaintiffs bring this Cause of Action on behalf of the California Sub-Class.

SIXTH CAUSE OF ACTION

VIOLATION OF STATE DATA BREACH LAWS
(On Behalf Of Plaintiffs And All Multi-State Sub-Class Members)

123. Plaintiffs repeat each and every allegation of this Complaint as if fully set forth at length herein.

124. Pursuant to materially identical data breach statutes of Alaska, Arkansas, California, Colorado, Connecticut, Delaware, Washington D.C., Florida, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maryland, Massachusetts, Michigan, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, North Carolina, North Dakota, Oklahoma, Oregon, Rhode Island, South Carolina, Tennessee, Texas, Utah, Virginia, Washington, Wisconsin, and Wyoming, Defendant is a business that collects and maintains PII of Plaintiffs and Class Members.

125. Defendant is responsible for reasonably safeguarding the PII of Plaintiffs and Class Members and to provide prompt notice of a data breach affecting such PII, consistent with the requirements of these materially identical state laws.

126. Defendant failed to safeguard, maintain, and/or dispose of the PII of Plaintiffs and Class Members as required by state law, and Plaintiffs and Class Members were injured, as described above, by Defendant's failure to do so.

127. Defendant failed to provide reasonable and timely notice of the Data Breach to Plaintiffs and Class Members, in violation of the following state data breach statutes:

a. Alaska Stat. Ann. § 45.48.010(a), *et seq*.;

b. Ark. Code Ann. § 4-110-105(a), et seq.;
c. Cal. Civ. Code § 1798.80, et seq.;
d. Colo. Rev. Stat. Ann § 6-1-716(2), et seq.;
e. Conn. Gen. Stat. Ann. § 36a-701b(b), et seq.;
f. Del. Code Ann. Tit. 6 § 12B-102(a), et seq.;
g. D.C. Code § 28-3852(a), et seq.;
h. Fla. Stat. Ann. § 501.171(4), et seq.;
i. Ga. Code Ann. § 10-1-912(a), et seq.;
j. Haw. Rev. Stat. § 487N-2(a), et seq.;
k. Idaho Code Ann. § 28-51-105(1), et seq.;
l. Ill. Comp. Stat. Ann. 530/10(a), et seq.;
m. Iowa Code Ann. § 715C.2(1), et seq.;
n. Kan. Stat. Ann. § 50-7a02(a), et seq.;
o. Ky. Rev. Stat. Ann. § 365.732(2), et seq.;
p. La. Rev. Stat. Ann. § 51:3074(A), et seq.;
q. Md. Code Ann., Commercial Law § 14-3504(b), et seq.;
r. Mass. Gen. Laws Ann. Ch. 93H § 3(a), et seq.;
s. Mich. Comp. Laws Ann. § 445.72(1), et seq.;
t. Minn. Stat. Ann. § 325E.61(1)(a), et seq.;
u. Mont. Code Ann. § 30-14-1704(1), et seq.;
v. Neb. Rev. Stat. Ann. § 87-803(1), et seq.;
w. Nev. Rev. Stat. Ann. § 603A.220(1), et seq.;
x. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), et seq.;
y. N.J. Stat. Ann. § 56:8-163(a), et seq.;
z. N.C. Gen. Stat. Ann. § 75-65(a), et seq.;
aa. N.D. Cent. Code Ann. § 51-30-02, et seq.;
bb. Okla. Stat. Ann. Tit. 24 § 163(A), et seq.;
cc. Or. Rev. Stat. Ann. § 646A.604(1), et seq.;

dd. R.I. Gen. Laws Ann. § 11-49.3-4(a)(1), et seq.;

ee. S.C. Code Ann. § 39-1-90(A), et seq.;

ff. Tenn. Code Ann. § 47-18-2107(b), et seq.;

gg. Tex. Bus. & Com. Code Ann. § 521.053(b), et seq.;

hh. Utah Code Ann. § 13-44-202(1), et seq.;

ii. Va. Code. Ann. § 18.2-186.6(B), et seq.;

jj. Wash. Rev. Code Ann. § 19.255.010(1), et seq.;

kk. Wis. Stat. Ann. § 134.98(2), et seq.; and

ll. Wyo. Stat. Ann. § 40-12-502(a), et seq.

128. As a direct and proximate result of Defendant's violations of the CRA, Plaintiffs and the Multi-State Sub-Class sustained actual losses and damages as described herein.

SEVENTH CAUSE OF ACTION

VIOLATION OF THE CALIFORNIA CONSUMER RECORDS ACT CAL. CIV. CODE §§ 1798.80, *ET SEQ.*

(On Behalf Of Plaintiffs And All California Sub-Class Members)

129. Plaintiffs repeat each and every allegation of this Complaint as if fully set forth at length herein.

130. Plaintiffs hereby plead in the alternative to the Sixth Cause of Action.

131. The California Legislature enacted the California Consumer Records Act ("CRA"), Cal. Civ. Code §§ 1798.80, *et seq*., "to ensure that Personal Information about California residents is protected." Cal. Civ. Code § 1798.81.5(a)(1).

132. The CRA requires that "[a] business that owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure." Cal. Civ. Code § 1798.81.5(b).

133. Defendant maintains computerized data that includes PII, as defined by Cal. Civ. Code § 1798.80. This includes PII about Plaintiffs and California Sub-Class Members, including, *inter alia*, their full names and SSNs. Cal. Civ. Code § 1798.81.5(d)(1)(A); Cal. Civ. Code § 1798.82.

134. Pursuant to the CRA, Defendant was required to "notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b). The security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82.

135. Defendant reasonably believed that Plaintiffs' and the California Sub-Class Members' PII was acquired by unauthorized persons during the Data Breach. As such, Defendant had an obligation under the CRA to disclose the Data Breach, immediately following its discovery, to Plaintiffs and California Sub-Class Members as the owners or licensees of the PII. Cal. Civ. Code § 1798.82.

136. By willfully, intentionally, and/or recklessly failing to disclose the Data Breach immediately following its discovery, Defendant violated Cal. Civ. Code § 1798.82.

137. As a direct and proximate result of Defendant's violations of the CRA, Plaintiffs and the California Sub-Class sustained actual losses and damages as described herein.

138. Plaintiffs and the California Sub-Class seek damages, injunctive relief, and other and further relief as the Court may deem just and proper.

EIGHTH CAUSE OF ACTION

VIOLATIONS OF THE CALIFORNIA CONSUMER PRIVACY ACT
Cal. Civ. Code §§ 1798.100 *et seq.* ("CCPA")
(On Behalf Of Plaintiffs And All California Sub-Class Members)

139. Plaintiffs repeat each and every allegation of this Complaint as if fully set forth at length herein.

140. This claim in pleaded on behalf of Plaintiff and the California Sub-Class.

141. In 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on certain businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected.

142. CPK is subject to the CCPA and failed to implement such procedures which resulted in the Data Breach.

143. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

144. Plaintiffs are "consumers" as defined by Civ. Code § 1798.140(g) because they are natural persons residing in the state of California.

145. Defendant is a "business" as defined by Civ. Code § 1798.140(c) because it is a corporation that does business in the state of California and has annual revenues of in excess of $25,000,000.

146. The CCPA provides that "personal information" includes "[a]n individual's first name or first initial and the individual's last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted . . . (i) Social Security number. *See* Civ. Code § 1798.150(a)(1); Civ. Code § 1798.81.5(d)(1)(A).

147. Plaintiffs' name in combination with SSNs, and other sensitive PII, compromised in the Data Breach constitutes "personal information" within the meaning of the CCPA.

148. Through the Data Breach, Plaintiffs' PII was accessed without authorization, exfiltrated, and stolen by criminals in a nonencrypted and/or nonredacted format

149. The Data Breach occurred as a result of Defendant's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

150. On December 10, 2021, Plaintiffs sent written notice to Defendant pursuant to Cal. Civ. Code § 1798.150(b)(1), identifying the specific provisions of the CCPA Plaintiffs allege Defendant has violated or is violating. Although a cure is not possible under the circumstances, if (as expected) Defendant is unable to cure or does not cure the violation within 30 days, Plaintiffs will amend this Complaint to pursue actual or statutory damages as permitted by Cal. Civ. Code § 1798.150(a)(1)(A).

151. As a result of Defendant's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiffs seek actual pecuniary damages, injunctive and declaratory relief, and any other relief as deemed appropriate by the Court.

NINTH CAUSE OF ACTION

DECLARATORY RELIEF
(On Behalf Of Plaintiffs And All Class Members)

152. Plaintiffs repeat each and every allegation of this Complaint as if fully set forth at length herein.

153. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court may enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Moreover, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

154. Defendant owes duties of care to Plaintiffs and Class Members, requiring it to reasonably and adequately secure their PII through sufficient data security policies, practices, and measures.

155. Defendant is still in possession of Plaintiffs' and Class Members' PII.

156. Plaintiffs allege that Defendant's data security policies, practices, and measures remain unreasonable and inadequate to secure Plaintiffs' and Class Members' PII.

157. Plaintiffs and Class Members continue to suffer injury as a result of Defendant's negligent exposure of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

158. Additionally, Plaintiffs' and Class Members' PII, when contained in electronic form, is highly attractive to criminals who can nefariously use their PII for fraud, identity theft, and other crimes without their knowledge and consent.

159. Plaintiffs seek a judgment declaring:

a. That Defendant owes a legal duty to reasonably and adequately secure Plaintiffs' and Class Members' PII.

b. That Defendant's past and present data security policies, practices, and measures do not comply with its contractual obligations and duties of care to reasonably and adequately secure Plaintiffs' and Class Members' PII.

c. That Defendant continues to breach its contractual obligations and duties of care by failing to implement reasonable and adequate data security policies, practices, and measures to safeguard Plaintiffs' and Class Members' PII.

160. Plaintiffs further seek an injunction from this Court compelling Defendant to implement cyber-security policies and procedures equal to or better than industry standards.

161. As alleged herein, the failures of the Defendant to implement adequate cyber-security measures and protocols has led to the compromise of the PII Plaintiffs and members of the Class were required to provide as a condition of obtaining educational services from Defendant, resulting in irreparable harm.

162. Defendant remains in possession of the PII of Plaintiffs and the Class. It is imperative that the Court intervene to assure that the Defendant takes all reasonable steps to protect that PII lest there be another data breach.

163. The hardship to Plaintiffs and Class Members if such an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Absent an injunction, Plaintiffs will likely be subjected to substantial identity theft and other damage, whereas the cost to CPK of complying with an injunction by employing reasonable data security policies, practices, and measures is relatively minimal, and CPK has a pre-existing legal obligation to employ such measures.

164. Issuance of the requested injunction will further relevant public interest, benefitting the public by preventing another data breach at CPK, thus eliminating the additional injuries that would result to Plaintiffs and other current and former employees whose PII would be further compromised.

165. Plaintiffs and the Class have no other adequate remedy at law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Aviva Kirsten and Jeremy Pittman demand judgment on behalf of themselves and the Class as follows:

a. Certifying that the action may be maintained as a class action and appointing the named Plaintiffs to be class representatives and the undersigned counsel to be Class counsel;

b. Requiring that Defendant pay for notifying the members of the Class of the pendency of this suit;

c. Awarding Plaintiffs and the Class appropriate relief, including actual damages, compensatory damages, and punitive damages on the First, Second, Third, Fourth, Fifth, Sixth, and Seventh Causes of Action;

d. Awarding injunctive relief on the Eighth Cause of Action requiring Defendant to safeguard the PII of all persons providing such information to Defendant it as part of and as a condition of employment with Defendant;

e. Awarding Plaintiffs and the Class prejudgment and post-judgment interest;

f. Awarding Plaintiffs and the Class their attorneys' fees and costs pursuant to applicable laws, together with their costs and disbursements of this action; and

g. Awarding such other and further relief as the Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiffs, individually and on behalf of the Class, demand a trial by jury as to all issues triable of right.

DATED: December 10, 2021

Respectfully submitted,

/s/ Tina Wolfson
Tina Wolfson (SBN 174806)
twolfson@ahdootwolfson.com
Theodore W. Maya (SBN 223242)
tmaya@ahdootwolfson.com
Deborah De Villa (SBN 312564)
ddevilla@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, California 91505
Tel. (310) 474.9111
Fax: (310) 474.8585

Todd. S. Garber (*pro hac vice* to be filed)
tgarber@fbfglaw.com
Andrew C. White (*pro hac vice* to be filed)
awhite@fbfglaw.com
FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP
One North Broadway, Suite 900
White Plains, New York 10601
Tel: (914) 298-3281
Fax: (914) 824-1561

Seth A. Meyer (*pro hac vice* to be filed)
sam@kellerlenkner.com
Alex J. Dravillas (*pro hac vice* to be filed)
ajd@kellerlenkner.com
KELLER LENKNER LLC
150 N. Riverside Plaza, Suite 4270
Chicago, IL 60606
Tel: (312) 741-5220

Counsel to Plaintiffs and the Proposed Class