Christopher L. Rudd (SBN 130713)
E-mail: clrudd@ruddlawla.com
S. Martin Keleti (SBN 144208)
E-mail: s.martin.keleti@gmail.com
THE RUDD LAW FIRM
4650 Sepulveda Boulevard, Suite 205
Sherman Oaks, CA 91403
Phone: (310) 633-0705
Fax: (310) 359-0258

Danielle L. Perry (SBN 292120)
E-mail: dperry@masonllp.com
MASON LIETZ & KLINGER LLP
5101 Wisconsin Avenue NW, Suite 305
Washington, DC 20016
Phone: (202) 429-2290
Fax: (202) 429-2294

Counsel for Plaintiffs and the Putative Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

DOUG WALLACE and ALONDRA MEZA, individually and on behalf of all others similarly situated, Plaintiffs, v. CALIFORNIA PIZZA KITCHEN, INC., a Delaware corporation, Defendant.	Case No. 8:21-cv-01970 **CLASS ACTION COMPLAINT FOR:** **1. NEGLIGENCE;** **2. NEGLIGENCE *PER SE*;** **3. BREACH OF IMPLIED CONTRACT;** **4. BREACH OF CONFIDENCE;** 5. **UNFAIR BUSINESS PRACTICES:** **DEMAND FOR JURY TRIAL**

Plaintiffs Doug Wallace and Alondra Meza (collectively, "Plaintiffs") bring this Class Action Complaint against Defendant California Pizza Kitchen, Inc. ("CPK") each in their individual capacity and on behalf of all others similarly situated (the "Class," defined below), and allege, upon personal knowledge as to their own actions and their counsel's investigation, and upon information and belief as to all other matters, as follows:

SUBJECT MATTER JURISDICTION

1. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). There are at least 100 putative Class Members; the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of interest and costs; and members of the proposed Class are citizens of states different from CPK

NATURE OF THE ACTION

2. This class action arises out of the recent targeted cyber-attack against CPK that allowed a third party to access CPK's computer systems and data (the "Cyber-Attack"), resulting in the compromise of highly sensitive personal information belonging to tens of thousands of current and former employees and their family members (the "Data Breach").

3. As a result of the Cyber-Attack, Plaintiffs and Class Members suffered ascertainable injury and damages in the form of the substantial and present risk of fraud and identity theft from their unlawfully accessed and compromised private and confidential information (including Social Security numbers), lost value of their private and confidential information, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Cyber-Attack.

4. Sensitive personal information of Plaintiffs and Class Members—which had been entrusted to CPK, it officers and agents—was compromised, unlawfully accessed, and stolen due to the Cyber-Attack. Information compromised in the Cyber-Attack includes the following: full name and Social Security number (collectively, the "Private Information").

5. Plaintiffs bring this class action lawsuit on behalf of all those similarly situated to address CPK's inadequate safeguarding of Class Members' Private Information that CPK collected and maintained.

6. CPK maintained the Private Information in a reckless manner. In particular, CPK maintained the Private Information CPK's computer network in a

condition vulnerable to cyber-attacks of this type.

7. The mechanism of the Cyber-Attack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known and foreseeable risk to CPK, and CPK was on notice that failing to take steps necessary to secure the Private Information from those risks left the Private Information in a dangerous condition.

8. In addition, CPK and its employees failed to properly monitor the computer network and systems that housed the Private Information. The Cyber-Attack occurred prior to September 15, 2021, and was discovered on October 4, 2021. Had CPK properly monitored its computer network and systems, it would have discovered the intrusion sooner.

9. Plaintiffs' and Class Members' identities are now at risk because of CPK's negligent conduct because the Private Information that CPK collected and maintained is now in the hands of data thieves.

10. Armed with the Private Information accessed in the Cyber-Attack, data thieves can commit a variety of crimes against Plaintiffs and Class Members, including, *e.g.*, opening new financial accounts in the names of Plaintiffs and Class Members; taking out loans in the names of Plaintiffs and Class Members; using the Private Information of Plaintiffs and Class Members to obtain government benefits; filing fraudulent tax returns using the Private Information of Plaintiffs and Class Members; obtaining driver licenses in the names of Plaintiffs and Class Members but substituting their photographs with those of other persons;, and giving false information to police during an arrest.

11. As a further result of the Cyber-Attack, Plaintiffs and Class Members have been exposed to a substantial and present risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

12. Plaintiffs and Class Members have and may also incur out of pocket

costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

13. As a direct and proximate result of the Cyber-Attack and subsequent Data Breach, Plaintiffs and Class Members have suffered and will continue to suffer damages and economic losses in the form of: 1) the loss of time needed to take appropriate measures to avoid unauthorized and fraudulent charges; change their usernames and passwords on their accounts; investigate, correct and resolve unauthorized debits; deal with spam messages and e-mails received subsequent to the Data Breach; and 2) charges, and fees charged against their accounts. Plaintiffs and Class Members have likewise suffered and will continue to suffer an invasion of their property interest in their own personally identifying information ("PII") such that they are entitled to damages for unauthorized access to and misuse of their PII from CPK, and Plaintiffs and Class Members will suffer from future damages associated with the unauthorized use and misuse of their PII as thieves will continue to use the stolen information to obtain money and credit in their name for several years.

14. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or removed from the network during the Cyber-Attack.

15. Plaintiffs seek remedies including, but not limited to, compensatory damages, nominal damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to CPK's data security systems, future annual audits, and adequate credit monitoring services funded by CPK.

16. Accordingly, Plaintiffs bring this action against CPK seeking redress for their unlawful conduct asserting claims for negligence, negligence *per se*, and breach of implied contract.

PARTIES

17. Plaintiff Doug Wallace ("Wallace") is an individual, a citizen

residing in Riverside County, California. Plaintiff Wallace was employed by CPK as a General Manger from February, 2000, to October, 2014. On or about November 15, 2021, Plaintiff Wallace received notice from CPK that the Data Breach had occurred following a security "incident," and that his personal data (including his name and Social Security number) were involved. A copy of the notice is attached as **Exhibit A** and incorporated by reference.

18. Plaintiff Alondra Meza ("Meza") is an individual, a citizen residing in Las Vegas, Nevada. Plaintiff Meza was employed by CPK as a Takeout Specialist from October, 2019, to September, 2020. On or about November 15, 2021, Plaintiff Meza received notice from CPK that the Data Breach had occurred following a security "incident," and that her personal data (including her name and Social Security number) was involved. A copy of the notice is attached as **Exhibit B** and incorporated by reference.

19. Defendant California Pizza Kitchen, Inc. ("CPK") is a Delaware corporation with its principal place of business at 575 Anton Boulevard, Suite 100, Costa Mesa, California, 92626. This Court has jurisdiction over CPK through its business operations in this District, the specific nature of which occurs in this District. CPK intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

VENUE

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District, and because CPK's principal place of business is located in this District.

FACTUAL ALLEGATIONS COMMON TO ALL CLAIMS

Defendant's Business

21. CPK is a global brand serving California cuisine in nearly 200

restaurants worldwide, 12 international cities, and 8 countries and U.S. territories.[1]

22. In the ordinary course of doing business with CPK, current and former employees provide CPK with sensitive, personal and private information such as:

- Name;
- Address;
- Phone number;
- Driver license number;
- Social Security number;
- Date of birth;
- Email address;
- Gender.

23. Plaintiffs and Class Members, as current and former employees, relied on CPK to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII.

24. CPK had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties.

The Cyber-Attack and Data Breach

25. On or about November 15, 2021, CPK began notifying current and former employees and state Attorneys General about a data breach that occurred prior to September 15, 2021 (the "Data Breach"). *See* Exhibits A & B (Plaintiffs' Notice of Data Breach letters).

26. According to the Notice of Data Breach letters CPK sent to Plaintiffs and letters CPK sent to state Attorneys General, CPK's security team learned of a potential security incident on September 15, 2021, and on October 4, 2021, after

[1] https://www.cpk.com/about (last accessed Nov. 26, 2021).

retaining a forensic specialist, confirmed that its systems had been subject to unauthorized access. *Id.*

27. CPK informed Plaintiffs that their full names and Social Security numbers may have been exfiltrated. *Id.*

28. The Notice of Data Breach letters offered a complementary twelve-month membership to Experian's IdentityWorks credit monitoring service.

29. Based on the Notice of Data Breach letters they received, which informed Plaintiffs that their Private Information was accessed on CPK's network and computer systems, and other publicly available information, Plaintiffs believe their names and Social Security numbers were stolen from CPK's network and subsequently sold on the dark web.

30. CPK had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

31. Plaintiffs and Class Members provided their Private Information to CPK with the reasonable expectation and mutual understanding that CPK would comply with its obligations to keep Private information confidential and secure from unauthorized access.

32. CPK's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches preceding the date of the breach.

33. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[2]

34. Indeed, cyber-attacks, such as the one experienced by CPK, have

[2] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed Dec. 10, 2020).

become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in CPK's industry, including CPK.

Plaintiffs' Exposure and Mitigation Efforts

Plaintiff Wallace

35. As a direct result of the Data Breach, Plaintiff Wallace has engaged in mitigation efforts and expended time and resources.

36. Subsequent to the Data Breach, Plaintiff Wallace subscribed to a credit monitoring service at the cost of $20 per month.

37. Subsequent to the Data Breach, Plaintiff Wallace now regularly checks his credit reports as well as his banking statements and credit card statements several times a week. This is time Plaintiff Wallace otherwise would have spent performing other activities, such as his working or leisure activities.

38. Knowing that thieves stole his PII and knowing that this information may now, or in the future, be available for sale on the dark web has caused Plaintiff Wallace anxiety. He is now very concerned about identity theft in general. This Data Breach has given Plaintiff Wallace hesitation about using electronic services and reservations about conducting other online activities requiring his PII.

39. Prior to receiving the Notice of Data Breach letter from CPK, Plaintiff Wallace had not received a Notice of Data Breach letter from any other company.

40. Plaintiff Wallace suffered actual injury from having his PII exposed as a result of the Data Breach including, but not limited to: (a) unauthorized credit card charges; (b) entrusting his PII to CPK which he would not have, had CPK disclosed that it lacked data security practices adequate to safeguard consumers'

PII from theft; (c) damages to and diminution in the value of his PII—a form of intangible property that Plaintiff Wallace entrusted to CPK as a condition of employment; (d) loss of his privacy; (e) present injury arising from the increased risk of fraud and identity theft; and (f) the time and expense of his mitigation efforts as a result of the Data Breach.

41. As a result of the Data Breach, Plaintiff Wallace will continue to be at heightened risk for financial fraud and identity theft, and the attendant damages, for years to come.

Plaintiff Meza

42. As a direct result of the Data Breach, Plaintiff Meza has engaged in mitigation efforts and expended time and resources.

43. Subsequent to the Data Breach, Plaintiff Meza experienced a substantial increase in spam emails, texts and phone calls.

44. Subsequent to the Data Breach, Plaintiff Meza now regularly checks her credit reports as well as her banking statements and credit card statements several times a week. This is time Plaintiff Meza otherwise would have spent performing other activities, such as her working or leisure activities.

45. Knowing that thieves stole her PII and knowing that this information may now, or in the future, be available for sale on the dark web has caused Plaintiff Meza anxiety. She is now very concerned about identity theft in general. This Data Breach has given Plaintiff Meza hesitation about using electronic services and reservations about conducting other online activities requiring her PII.

46. Prior to receiving the Notice of Data Breach letter from CPK, Plaintiff Meza had not received a Notice of Data Breach letter from any other company.

47. Plaintiff Meza suffered actual injury from having her PII exposed as a result of the Data Breach including, but not limited to: (a) entrusted her PII to CPK

that she would not have had CPK disclosed that it lacked data security practices adequate to safeguard consumers' PII from theft; (b) damages to and diminution in the value of her PII—a form of intangible property that Plaintiff Meza entrusted to CPK as a condition of employment; (c) loss of her privacy; (d) imminent and impending injury arising from the increased risk of fraud and identity theft; and (d) the time and expense of his mitigation efforts as a result of the Data Breach.

48. As a result of the Data Breach, Plaintiff Meza will continue to be at heightened risk for financial fraud and identity theft, and the attendant damages, for years to come.

CPK's Failure to Comply with FTC Guidelines

49. The Federal Trade Commission ("FTC") promulgates numerous guides for businesses highlighting the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[3]

50. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[4] The guidelines note that businesses should protect the personal customer information they keep; properly dispose of PII that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

51. The FTC further recommends companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry–tested methods for security; monitor for suspicious activity on the network; and verify third–party

[3] Federal Trade Commission, *Start With Security*, *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed Sept. 9, 2021).

[4] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Sept. 9, 2021).

service providers have implemented reasonable security measures.[5]

52. The FTC brings enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

53. CPK failed to properly implement basic data security practices. CPK's failure to employ reasonable and appropriate measures to protect against unauthorized access to members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

54. CPK was at all times fully aware of its obligation to protect Plaintiffs' and Class Members' PII because of CPK's position as Plaintiffs' and Class Members' employer. CPK was also aware of the significant repercussions that would result from its failure to do so.

CPK's Failure to Comply with Industry Standards

55. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing CPK's cybersecurity practices.

56. Best cybersecurity practices that are standard in the food service industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

57. Upon information and belief, CPK failed to meet the minimum

[5] FTC, *Start With Security*, *supra* note 17.

standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

58. These foregoing frameworks are existing and applicable industry standards in CPK's industry, and CPK failed to comply with these accepted standards, thereby opening the door to the Cyber-Attack and causing the data breach.

CPK's Breach

59. CPK breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems, networks, and data. CPK's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

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

b. Failing to adequately protect current and former employees' Private Information;

c. Failing to adequately protect Private Information of current and former employees' family members;

d. Failing to properly monitor its own data security systems for existing intrusions, brute-force attempts, and clearing of event logs;

e. Failing to apply all available security updates;

f. Failing to install the latest software patches, update its firewalls, check user account privileges, or ensure proper security practices;

g. Failing to practice the principle of least-privilege and maintain credential hygiene;

h. Failing to avoid the use of domain-wide, administrator-level service accounts;

i. Failing to employ or enforce the use of strong randomized, just-in-time local administrator passwords; and

j. Failing to properly train and supervise employees in the proper handling of inbound emails.

60. As the result of computer systems in need of security upgrading and inadequate procedures for handling cybersecurity threats, CPK negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information.

Data Breaches Put Victims at a Present Increased Risk of Fraud and Identity Theft

61. CPK understood the Private Information it collected is highly sensitive, and of significant value to those who would use it for wrongful purposes, such as the cyber-criminals who perpetrated this Cyber-Attack.

62. The United States Government Accountability Office released a report in 2007 regarding data breaches (the "GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[6]

63. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their

[6] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 12, 2019) (the "GAO Report").

accounts, placing a credit freeze on their credit, and correcting their credit reports.[7]

64. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

65. Identity thieves can also use Social Security numbers to obtain a driver license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

66. In addition, identity thieves may obtain a job using the victim's Social Security number, 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.

67. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[8]

68. The value of personal data is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

69. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [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.

[7] *See* https://www.identitytheft.gov/Steps (last visited Dec. 8, 2020).
[8] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last accessed Dec. 10, 2020).

> As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report at 29.

70. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

71. Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground Internet websites.

72. Where the most private information belonging to Plaintiffs and Class Members was accessed and removed from CPK's network, and entire batches of that stolen information already had been dumped by the cyberthieves on the cyber black market, there is a strong probability that additional batches of stolen information are yet to be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

73. Thus, Plaintiffs and Class Members must vigilantly monitor their financial accounts for many years to come.

74. Sensitive information can sell for as much as $363 according to the Infosec Institute. PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

75. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.

76. Social Security numbers are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration

stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.

77. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

78. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[9]

79. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[10]

80. At all relevant times, CPK knew or reasonably should have known

[9] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Feb. 9, 2015, http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited Oct. 28, 2020).

[10] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Feb. 6, 2015, http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Oct. 28, 2020).

these risks, the importance of safeguarding Private Information, and the foreseeable consequences if its data security systems were breached and strengthened their data systems accordingly. CPK was put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

Plaintiffs' and Class Members' Damages

81. The ramifications of CPK's failure to keep Plaintiffs' and Class Members' PII secure are long lasting and severe. Once that kind of information is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[11]

82. The PII belonging to Plaintiffs and Class Members is private, sensitive in nature, and left inadequately protected by CPK—who did not obtain Plaintiffs' or Class Members' consent to disclose such information to any other person as required by applicable law and industry standards.

83. The Data Breach was a direct and proximate result of CPK's failure to: (a) properly safeguard and protect Plaintiffs' and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PII; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

84. CPK had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect member data.

[11] *2014 LexisNexis True Cost of Fraud Study, available at:* https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last accessed Sept. 9, 2021).

85. CPK could have prevented the intrusions into its systems and, ultimately, the theft of PII if CPK had remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field.

86. As a direct and proximate result of CPK's wrongful actions and inactions, Plaintiffs and Class Members are now in imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to dedicate time and resources which they otherwise would have dedicated to other life demands, such as work and family, to mitigate the actual and potential impact of the Data Breach on their lives.

87. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had PII or PHI used for fraudulent purposes, 29% spent a month or more resolving problems," and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[12]

88. In the breach notification letter, CPK made an offer of 12–months of identity monitoring services to its patients. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, medical and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' PII.

89. As a direct result of CPK's failures to prevent the Data Breach, Plaintiffs and Class Members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their PII;

b. Out–of–pocket costs associated with the prevention, detection,

[12] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed Sept. 9, 2021).

recovery, and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and loss of productivity from addressing and attempting to mitigate actual and future consequences of the Data Breach, including but not limited to researching how to prevent, detect, contest, and recover from identity theft and fraud;

d. The present and continued risk to their PII, which remains in the possession of CPK and is subject to further breaches so long as CPK fails to undertake appropriate measures to protect the PII in its possession; and

e. Current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

90. In addition to a remedy for the economic harm, Plaintiffs and Class Members maintain an undeniable interest in ensuring their PII is secure, remains secure, and is not subject to further misappropriation and theft.

91. As a direct and proximate result of CPK's actions and inactions, Plaintiffs and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

CLASS ACTION ALLEGATIONS

92. Plaintiffs bring this suit on behalf of themselves and a class and state subclasses of similarly situated individuals under Federal Rule of Civil Procedure 23, which are preliminarily defined as:

a. All persons whose PII stored or possessed by CPK was subject to the Data Breach announced by CPK on or about November 15, 2021 (the "Class").

b. All residents of the State of California whose PII stored or possessed

by CPK was subject to the Data Breach announced by CPK on or about November 15, 2021 (the "California Subclass").

c. All residents of the State of Nevada whose PII stored or possessed by CPK was subject to the Data Breach announced by CPK on or about November 15, 2021 (the "Nevada Subclass") (Plaintiffs refer to the California Subclass and the Nevada Subclass collectively as the "State Subclasses").

93. Excluded from the Class are the following individuals and/or entities: CPK and CPK's parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which CPK has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; Class counsel; and all judges assigned to hear any aspect of this litigation, as well as their staff and immediate family members.

94. Plaintiffs reserve the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

95. **Numerosity:** The Class is so numerous that joinder of all members is impracticable. CPK has identified more than 100,000 persons whose PII may have been improperly accessed in the Data Breach, and the Class is identifiable within CPK's records. A precise number of class members can be ascertained through appropriate discovery and from records maintained by CPK.

96. **Commonality and Predominance:** Questions of law and fact common to the Class exist and predominate over any questions affecting only individual Class members. These include but are not limited to, the following:

a. Whether Plaintiffs' and the Class members' PII was accessed and/or viewed by one or more unauthorized persons in the Data Breach

alleged above;

b. Whether CPK's publishing Plaintiffs' and Class members' PII to unauthorized persons was permissible without the prior written authorization of the Plaintiffs or the Class members;

c. When and how CPK should have learned and actually learned of the Data Breach;

d. Whether CPK's response to the Data Breach was adequate;

e. Whether CPK owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their PII;

f. Whether CPK breached that duty;

g. Whether CPK implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiffs' and Class members' PII;

h. Whether CPK acted negligently in connection with the monitoring and/or protecting of Plaintiffs' and Class members' PII;

i. Whether CPK knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and Class members' PII secure and prevent loss or misuse of that PII;

j. Whether CPK adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

k. Whether CPK caused Plaintiffs and Class members damages;

l. Whether CPK violated the law by failing to promptly notify Plaintiffs and Class members that their PII was compromised;

m. Whether Plaintiffs and Class members are entitled to actual damages, nominal and/or statutory damages, credit monitoring, other monetary relief, and/or equitable relief; and

n. Whether CPK violated the California Unfair Competition Law (Business & Professions Code § 17200 *et seq*.).

97. There are no defenses of a unique nature that may be asserted against the Plaintiffs individually, as distinguished from the other Class Members, and the relief sought is common to the Class.

98. **Typicality:** Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised because of the Data Breach, due to CPK's identical conduct.

99. **Adequacy of Representation:** Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that Plaintiffs' interests are aligned with the class. Plaintiffs have no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. Plaintiffs seek no relief that is adverse to Class Members. In addition, Plaintiffs retained counsel experienced in data breach and complex consumer class action litigation. Neither Plaintiffs nor their counsel have any interests which might cause them not to vigorously pursue this claim.

100. **Superiority:** Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain class members, who could not individually afford to litigate a complex claim against large entities, such as CPK. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

101. The prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudications with respect to individual members of the Class, and a risk that any adjudications with respect to individual members of the Class would, as a practical matter, either be dispositive

of the interests of other members of the Class not party to the adjudication or substantially impair or impede their ability to protect their interests.

102. Class certification is also warranted for purposes of injunctive and declaratory relief because CPK has acted, or refused to act, on grounds generally applicable to the class, so that final injunctive and declaratory relief are appropriate with respect to the Class as a whole.

CLAIMS FOR RELIEF

First Claim for Relief

Negligence

(On Behalf of Plaintiffs, the Class, or Alternatively the State Subclasses)

103. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 102 above as if fully set forth herein.

104. CPK's own negligent conduct created a foreseeable risk of harm to Plaintiffs and Class Members. CPK's negligence included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. CPK's negligence also included its decision not to comply with (1) industry standards, and/or best practices for the safekeeping and encrypted authorized disclosure of the PII of Plaintiffs and Class Members; or (2) Section 5 of the FTC Act.

105. First, CPK had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining and testing its security protocols to ensure PII in CPK's possession was adequately secured and protected, and that employees tasked with maintaining such information were adequately trained on relevant cybersecurity measures. CPK also had a duty to put proper procedures in place to prevent the unauthorized dissemination of Plaintiffs' and Class Members' PII.

106. As a condition of employment, Plaintiffs and Class Members were

obligated to provide CPK with their PII. As such, Plaintiffs and the Class Members entrusted their PII to CPK with the understanding CPK would safeguard their information.

107. CPK was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach. However, Plaintiffs and Class Members had no ability to protect their PII in CPK's possession.

108. CPK had full knowledge of the sensitivity of the PII, and the types of harm Plaintiffs and Class Members could, would, and will suffer if the information were wrongfully disclosed.

109. CPK admitted that its computer system containing Plaintiffs' and Class Members' PII was wrongfully compromised and accessed by unauthorized third persons, and that the Data Breach occurred due to CPK's actions and/or omissions.

110. Plaintiffs and Class Members were the foreseeable and probable victims of CPK's negligent and inadequate security practices and procedures that led to the Data Breach. CPK knew or should have known of the inherent risks in collecting and storing the highly valuable PII of Plaintiffs and Class Members, the critical importance of providing adequate security of that information, the current cyber security risks being perpetrated, and that CPK had inadequate employee training, monitoring and education and IT security protocols in place to secure the PII of Plaintiffs and Class Members.

111. CPK negligently, through its actions and/or omissions, and unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' PII while the information was within CPK's possession and/or control by failing to comply with and/or deviating from standard industry rules, regulations, and practices at the time of the Data Breach.

112. Second, CPK's violations of Section 5 of the FTC Act constitute

negligence. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as CPK, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of CPK's duty in this regard.

113. CPK violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and Class members' PII and not complying with applicable industry standards, as described in detail herein. CPK's conduct was particularly unreasonable given the nature and amount of PII it required, obtained, and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiffs and Class members.

114. Plaintiffs and Class Members are within the class of persons the FTC Act was intended to protect.

115. The harm the Data Breach caused, and continues to cause, is the type of harm the FTC Act was intended to guard against. The FTC pursues enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

116. CPK, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent unauthorized dissemination of Plaintiffs' and Class Members' PII.

117. CPK, through its actions and/or omissions, unlawfully breached its duty to adequately disclose to Plaintiffs and Class Members the existence and scope of the Data Breach.

118. But for CPK's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, Plaintiffs' and Class Members' PII would not have been compromised.

119. There is a temporal and close causal connection between CPK's failure to implement security measures to protect the PII and the harm suffered, and/or risk of present and continual harm suffered, by Plaintiffs and Class Members.

120. As a direct and proximate result of CPK's negligence, Plaintiffs and Class Members have suffered, and continue to suffer, injuries and damages arising from the Data Breach, including, but not limited to: damages from lost time and efforts to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, filing police reports, and damages from identity theft, which may take months—if not years—to discover, detect, and remedy.

121. Additionally, as a direct and proximate result of CPK's negligence, Plaintiffs and Class Members have suffered, and will continue to suffer, the continued risks of exposure of their PII, which remains in CPK's possession and is subject to further unauthorized disclosures so long as CPK fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

Second Claim for Relief

Negligence *Per Se*

(On Behalf of Plaintiffs, the Class, or Alternatively the State Subclasses)

122. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 102, and paragraphs 104 through 121 above as if fully set forth herein.

123. Pursuant to Section 5 of the FTC Act, 15 U.S.C. § 45, CPK had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

124. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

125. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act 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 and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

126. CPK breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

127. CPK's failure to comply with applicable laws and regulations constitutes negligence *per se.*

128. But for CPK's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

129. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of CPK's breach of its duties. CPK knew or should have known that it was failing to meet their duties, and that CPK's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

130. As a direct and proximate result of CPK's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

Third Claim for Relief

Breach of Implied Contract

(On Behalf of Plaintiffs, the Class, or Alternatively the State Subclasses)

131. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 102 above as if fully set forth herein.

132. Plaintiffs and Class Members were required to provide their PII, including their names and Social Security numbers to CPK as a condition of employment.

133. Plaintiffs and Class Members providing their PII and their labor to CPK in exchange for services, along with CPK's promise to protect their PII from unauthorized disclosure.

134. Upon information and belief, in its written privacy policies, CPK expressly promised Plaintiffs and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

135. Implicit in the agreement between Plaintiffs and Class Members on the one hand, and CPK on the other, regarding providing PII, was CPK's obligation to: (a) use such PII for business purposes only; (b) take reasonable steps to safeguard that PII; (c) prevent unauthorized disclosures of the PII; (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII; (e) reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses; and (f) retain the PII only under conditions that kept such information secure and confidential.

136. Without such implied contracts, Plaintiffs and Class Members would not have provided their PII to CPK.

137. Plaintiffs and Class Members fully performed their obligations under the implied contract with CPK. However, CPK did not.

138. CPK breached the implied contracts with Plaintiffs and Class members by failing to reasonably safeguard and protect Plaintiffs' and Class Members' PII, which was compromised as a result of the Data Breach.

139. As a direct and proximate result of CPK's breach of the implied contracts, Plaintiffs and Class Members have suffered, and continue to suffer, injuries and damages arising from the Data Breach including, but not limited to:

damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, filing police reports, and damages from identity theft, which may take months if not years to discover, detect, and remedy.

Fourth Claim for Relief

Breach of Confidence

(On Behalf of Plaintiffs, the Class, or Alternatively the State Subclasses)

140. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 102 above as if fully set forth herein.

141. At all times during Plaintiffs' and Class Members' interactions with CPK, CPK was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' PII that Plaintiffs and Class Members provided to CPK.

142. As alleged herein and above, CPK's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

143. Plaintiffs and Class Members provided their respective PII to CPK with the explicit and implicit understandings that CPK would protect and not permit the information to be disseminated to any unauthorized parties.

144. Plaintiffs and Class Members also provided their PII to CPK with the explicit and implicit understandings that CPK would take precautions to protect that PII from unauthorized disclosure, such as following basic principles of protecting its networks and data systems.

145. CPK required and voluntarily received, in confidence, Plaintiffs' and Class Members' PII with the understanding that the information would not be

disclosed or disseminated to the public or any unauthorized third parties.

146. Due to CPK's failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, following best information security practices to secure Plaintiffs' and Class Members' PII, Plaintiffs' and Class Members' PII was disclosed to, and misappropriated by, unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

147. As a direct and proximate cause of CPK's actions and/or omissions, Plaintiffs and Class Members have suffered, and will continue to suffer damages.

148. But for CPK's disclosure of Plaintiffs' and Class Members' PII in violation of the parties' understanding of confidence, Plaintiffs' and Class Members' PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. CPK's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' PII, as well as the resulting damages.

149. The injury and harm Plaintiffs and Class Members suffered, and continue to suffer, was the reasonably foreseeable result of CPK's unauthorized disclosure of Plaintiffs' and Class Members' PII. CPK knew its computer systems and technologies for accepting and securing Plaintiffs' and Class Members' PII had numerous security and other vulnerabilities placing Plaintiffs' and Class Members' PII in jeopardy.

150. As a direct and proximate result of CPK's breaches of confidence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent

researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in CPK's possession and is subject to further unauthorized disclosures so long as CPK fails to undertake appropriate and adequate measures to protect the PII in its continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (g) the diminished value of CPK's services they received.

151. As a direct and proximate result of CPK's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non–economic losses.

Fifth Claim for Relief

Violation of the California Unfair Competition Law,

Cal. Bus. & Prof. Code § 17200 *et seq*.--Unfair Business Practices

(On Behalf of Plaintiff Wallace and the California Subclass)

152. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 102 above as if fully set forth herein.

153. CPK violated California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq*. ("UCL"), by engaging in unlawful, unfair, or fraudulent business acts and practices, and unfair, deceptive, untrue, or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. & Prof. Code § 17200 with respect to the services provided to Plaintiff Wallace and California Subclass Members.

154. CPK engaged in unlawful acts and practices with respect to the services by establishing the sub–standard security practices and procedures described herein; by soliciting and collecting Plaintiff Wallace's and California Subclass Members' PII with knowledge the information would not be adequately protected; and by storing Plaintiff Wallace's and California Subclass Members' PII in an unsecure electronic environment in violation of California's data breach

statute, Cal. Civ. Code § 1798.81.5, which require CPK to take reasonable methods of safeguarding the PII of Plaintiff Wallace and California Subclass Members.

155. In addition, CPK engaged in unlawful acts and practices by failing to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

156. As a direct and proximate result of CPK's unlawful practices and acts, Plaintiff Wallace and California Subclass Members were injured and lost money or property, including but not limited to the price received by CPK for the services, the loss of Plaintiff Wallace's and California Subclass Members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described herein.

157. CPK knew or should have known CPK's computer systems and data security practices were inadequate to safeguard Plaintiff Wallace's and California Subclass Members' PII and that the risk of a data breach or theft was highly likely. CPK's actions in engaging in the above–named unlawful practices and acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of Plaintiff Wallace and the California Subclass Members.

158. Plaintiff Wallace, on behalf of the California Subclass, seeks relief under the UCL, including, but not limited to, restitution to Plaintiffs and California Subclass Members of money or property CPK may have acquired by means of CPK's unlawful, and unfair business practices, restitutionary disgorgement of all monies that accrued to CPK because of CPK's unlawful and unfair business practices, declaratory relief, attorney fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, request that the Court grant judgment against CPK as follows:

A. An order certifying the Class as defined herein, and appointing Plaintiffs and their Counsel to represent the Class;

B. Injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting CPK from engaging in the wrongful and unlawful acts described herein,

ii. requiring CPK to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws,

iii. requiring CPK to delete, destroy, and purge the PII of Plaintiffs and Class members unless CPK can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members,

iv. requiring CPK to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members,

v. prohibiting CPK from maintaining Plaintiffs' and Class Members' PII on a cloud-based database,

vi. requiring CPK to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on CPK's systems on a periodic basis, and ordering CPK to promptly correct any problems or issues detected by such

third-party security auditors,

vii. requiring CPK to engage independent third-party security auditors and internal personnel to run automated security monitoring,

viii. requiring CPK to audit, test, and train its security personnel regarding any new or modified procedures,

ix. requiring CPK to conduct regular database scanning and securing checks,

x. requiring CPK to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiffs and Class Members,

xi. requiring CPK to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach,

xii. requiring CPK to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with CPK's policies, programs, and systems for protecting PII,

xiii. requiring CPK to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor CPK's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated,

xiv. requiring CPK to meaningfully educate all Class Members about

the threats that they face as a result of the loss of their PII to third parties, as well as the steps affected individuals must take to protect themselves,

xv. requiring CPK to design, maintain, and test its computer systems to ensure that PII in its possession is adequately secured and protected,

xvi. requiring CPK disclose any future data disclosures in a timely and accurate manner; and

xvii. requiring CPK to provide ongoing credit monitoring and identity theft repair services to Class Members.

C. An award of compensatory, statutory, and nominal damages in an amount to be determined;

D. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of CPK's wrongful conduct;

E. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

F. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury.

Dated: December 2, 2021

/s/ *S. Martin Keleti*

Christopher L. Rudd (SBN 130713)
E-mail: clrudd@ruddlawla.com
S. Martin Keleti (SBN 144208)
E-mail: s.martin.keleti@gmail.com
THE RUDD LAW FIRM
4650 Sepulveda Boulevard, Suite 205
Sherman Oaks, CA 91403
Phone: (310) 633-0705
Fax: (310) 359-0258

Danielle L. Perry (SBN 292120)
E-mail: dperry@masonllp.com
MASON LIETZ & KLINGER LLP
5101 Wisconsin Avenue NW, Suite 305
Washington, DC 20016
Phone: (202) 429-2290
Fax: (202) 429-2294

Counsel for Plaintiffs and the Putative Class

ClassAction.org
