SIRI & GLIMSTAD LLP
Mason Barney (*pro hac vice* forthcoming)
mbarney@sirillp.com
Sonal Jain (*pro hac vice* forthcoming)
sjain@sirillp.com
200 Park Avenue
Seventeenth Floor
New York, NY 10166
Telephone: 212-532-1091
Facsimile: 646-417-5967

Nicholas Armer (Bar No. 330577)
narmer@sirillp.com
700 S Flower Street
Suite 1000
Los Angeles, CA 90017
Telephone: 212-532-1091
Facsimile: 646-417-5967

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

KANSAS GILLEO AND SYDNEY RUSEN, individually and on behalf of others similarly situated, Plaintiff, v. CALIFORNIA PIZZA KITCHEN, INC., and DOES 1-10, Defendants.	Case No. CLASS ACTION COMPLAINT FOR DAMAGES AND RELIEF AND DEMAND FOR JURY TRIAL COMPLAINT FOR 1. Negligence; 2. Negligence Per Se; 3. Declaratory judgment; 4. Violation of the New York General Business Law;

5. Violation of California Unfair Competition Law;
6. Violation of California Customer Records Act.

Plaintiffs KANSAS GILLEO and SYDNEY RUSEN, (each a "Plaintiff" and collectively "Plaintiffs") individually and on behalf of the Classes defined below of similarly situated persons, allege the following against Defendant CALIFORNIA PIZZA KITCHEN, INC. ("Defendant" or "CPK") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiffs bring this class action against CPK for its failure to properly secure and safeguard Plaintiffs' and other similarly situated CPK current and former employees' personal information from hackers.

2. CPK is a casual dining restaurant chain that specializes in California-style pizza.

3. On or about September 15, 2021, hackers gained access to the personally identifiable information ("PII") of over 100,000 current and former CPK employees (the "Data Breach"), including names, social security numbers, and possibly other PII.

4. On or about October 4, 2021, CPK determined that files on its systems had been subject to unauthorized access.

5. Thereafter, on or about November 15, 2021, CPK mailed written notice of the Data Breach to the affected current and former CPK employees (the "Class Members), including Plaintiffs.

6. Not only did hackers access the Class Members' PII, on information and belief, the PII is currently up for sale on the dark web. Hackers frequently offer for sale the unencrypted, unredacted, stolen PII to criminals. Because of Defendant's Data Breach, it is believed that the Class Members' PII is still available on the dark

web for criminals to access and abuse. As a result, the affected Class Members face a lifetime risk of identity theft.

7. Clearly, CPK failed to safeguard Plaintiffs' and the Class Members' PII and unreasonably delayed to inform them of the Data Breach.

8. Plaintiffs and the Class Members have suffered injury because of CPK's conduct. The injuries suffered by Plaintiffs and the proposed Classes as a direct result of the Data Breach include, *inter alia*:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft;

c. Costs associated with time spent and the loss of productivity from taking time to address and attempting to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals, which has already been misused via the sale of Plaintiffs' and the Class Members' information on the Internet black market;

e. Damages to and diminution in value of their PII entrusted to their employer, CPK, with the mutual understanding that Defendant would safeguard Plaintiffs' and the Class Members' data against theft and not allow access to and misuse of their PII by others;

f. Continued risk to their PII, which remains in the possession of CPK, and which is subject to further breaches so long as Defendant continues to fail to undertake appropriate and

adequate measures to protect Plaintiffs' and the Class Members' data in its possession.

9. Plaintiffs bring this action on behalf of all persons whose PII was compromised due to CPK's failure to: (i) adequately protect its users' PII, (ii) warn users of its inadequate information security practices, and (iii) effectively monitor its websites and e-commerce platforms for security vulnerabilities and incidents. CPK's conduct amounts to negligence and violates federal and state statutes.

II. JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. At least one member of the class is a citizen of a state different from CPK.

11. This Court has personal jurisdiction over CPK because it regularly conducts business in California, has sufficient minimum contacts in California, including its principal place of business, and intentionally avails itself of this jurisdiction by marketing and operating restaurants in California.

12. 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, including (upon information and belief) the Data Breach. CPK caused harm to Plaintiffs and the Class Members through its actions in this District. Additionally, CPK's principal place of business is located within the Central District of California.

III. PARTIES

13. Plaintiff Kansas Gilleo is a resident of New York. Plaintiff Gilleo is a former employee of the CPK location in Scarsdale, New York. On or around November 18, 2021, Plaintiff Gilleo received a letter from CPK informing her of the Data Breach and that her PII had been exposed.

14. Plaintiff Sydney Rusen is a resident of California. Plaintiff Rusen is a former employee of the CPK location in Santa Barbara, California. On November 18, 2021, Plaintiff Rusen received a letter from CPK informing her of the Data Breach and that her PII had been exposed.

15. Defendant California Pizza Kitchen, Inc. is a privately held corporation organized under the laws of the State of Delaware, with a principal place of business at 575 Anton Blvd., Suite 100, Costa Mesa, CA 92626. CPK advertises and operates restaurants throughout the United States. Its website can be found at the www.cpk.com URL, which is registered to California Pizza Kitchen, Inc. with a California address.[1]

IV. FACTUAL ALLEGATIONS

A. Background

16. CPK is a casual dining restaurant chain known for California-style pizza. It publicizes that "in Beverly Hills in 1985, former federal prosecutors Rick Rosenfield and Larry Flax combined their passion for food with fresh high-quality ingredients to create [CPK]."[2]

17. CPK is a global brand operating nearly 200 restaurants worldwide with over 14,000 employees.[3]

B. The Data Breach

18. CPK failed to prioritize data and cyber security by adopting reasonable data and cyber security measures to prevent and detect the unauthorized access to Plaintiffs' and the Class Members' PII.

[1] *See* https://www.whois.com/whois/cpk.com (last visited on November 19, 2021).

[2] *See* https://www.cpk.com/about(last visited on November 19, 2021).

[3] *Id*.

19. On or about November 15, 2021, CPK mailed a written notice of the Data Breach to Plaintiffs and the Class Members stating the following:

> On or about September 15, 2021, CPK learned of a disruption to certain systems on our computing environment. We immediately secured our environment and, with the assistance of leading third-party computer forensic specialists, launched an investigation to determine the nature and scope of the incident. On October 4, 2021, the investigation confirmed that certain files on our systems had been subject to unauthorized access.
>
> We therefore undertook a meticulous review of the potentially impacted files and our internal systems in order to identify the information that was involved and to whom it related. Unfortunately, on October 13, 2021, we determined that certain files containing your information could have been accessed during the event . . . .
>
> Our investigation determined that the information related to you that may have been affected includes your name and Social Security number.

20. Indeed, it appears that CPK did not even implement basic security measures despite Plaintiffs' and the Class Members' understanding that CPK: (i) would not disclose employees' PII; and (ii) would protect employees' PII with adequate security measures.

21. On information and belief, CPK employees' PII exposed in the Data Breach may currently be up for sale on the dark web. As a result, Plaintiffs and the Class Members face a lifetime risk of identity theft.

C. FTC and NIST Guidelines on Protecting Customer Personal Information

22. Recently, the Federal Trade Commission ("FTC") has held that the failure to employ reasonable measures to protect against unauthorized access to

confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTC Act ("FTCA") (codified by 15 U.S.C. § 45).

23. Under the FTCA, CPK is prohibited from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTCA.

24. Beginning in 2007, the FTC released a set of industry standards related to data security and the data security practices of businesses, called "Protecting Personal Information: A Guide for Businesses" (the "FTC Guide").[4] In 2011, this guidance was updated to include fundamental data security principles for businesses. In addition to the necessity to protect consumer data, the guide established that:

- Businesses should dispose of personal identifiable information that is no longer needed;
- Businesses should encrypt personal identifiable information and protected cardholder data stored on computer networks so that it is unreadable even if hackers are able to gain access to the information;
- Businesses should thoroughly understand the types of vulnerabilities on their network (of which malware on a point-of-sale system is one) and how to address said vulnerabilities;
- Businesses should implement protocols necessary to correct security breaches;

[4] *See FTC Unveils Practice Suggestions for Businesses on Safeguarding Personal Information*, FEDERAL TRADE COMM'N (Mar. 8, 2007), https://www.ftc.gov/news-events/press-releases/2007/03/ftc-unveils-practical-suggestions-businesses-safeguarding (last visited on November 19, 2021); *see also* Fed. Trade Comm'n, *Protecting Personal Information: A Guide for Business, Federal Trade Commission* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal information.pdf (updated FTC Guide) (last visited on November 19, 2021).

- Businesses should install intrusion detection systems to expose security breaches at the moment they occur;
- Businesses should install monitoring mechanisms to watch for massive troves of data being transmitted from their systems; and,
- Businesses should have an emergency plan prepared in response to a breach.

25. On information and belief, CPK failed to adequately address the foregoing requirements in the FTC Guide.

26. In 2015, the FTC supplemented the FTC Guide with a publication called "Start with Security" (the "Supplemented FTC Guide").[5] This supplement added further requirements for businesses that maintain customer data on their networks:

- Businesses should not keep personal identifiable information and protected cardholder data stored on their networks for any period longer than what is needed for authorization;
- Businesses should use industry-tested methods for data security; and,
- Businesses should be continuously monitoring for suspicious activity on their network.

27. Again, CPK apparently failed to adequately address these requirements enumerated in the Supplemented FTC Guide.

28. The FTC Guide is clear that businesses should, among other things: (1) protect the personal customer information they acquire; (2) properly dispose of personal information that is no longer needed; (3) encrypt information stored on computer networks; (4) understand their network's vulnerabilities; and (5)

[5] Fed. Trade Comm'n, Start with Security: A Guide for Business (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited on November 19, 2021).

implement policies for installing vendor-approved patches to correct security vulnerabilities. The FTC guidance also recommends that businesses: (1) use an intrusion detection system to expose a breach as soon as it occurs; (2) monitor all incoming traffic for activity indicating that someone may be trying to penetrate the system; and (3) watch for large amounts of data being transmitted from the system.[6] Plaintiffs believe that CPK did not follow these recommendations, and as a result exposed over 100,000 current and former CPK employees to harm.

29. Furthermore, the FTC has issued orders against businesses for failing to employ reasonable measures to safeguard customer data. The orders provide further public guidance to businesses concerning their data security obligations.

30. CPK knew or should have known about its obligation to comply with the FTCA, the FTC Guide, the Supplemented FTC Guide, and many other FTC pronouncements regarding data security.

31. Thus, among other things, CPK's misconduct violated the FTCA and the FTC's data security pronouncements, led to the Data Breach, and resulted in harm directly and proximately to Plaintiffs and the Class Members.

32. Additionally, the National Institute of Standards and Technology ("NIST") provides basic network security guidance that enumerates steps to take to avoid cybersecurity vulnerabilities.[7] Although use of NIST guidance is voluntary, the guidelines provide valuable insights and best practices to protect network systems and data.

[6] *See, e.g.*, *id.*; Fed. Trade Comm'n, *Protecting Personal Information: A Guide for Business* (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited on November 19, 2021).

[7] *Framework for Improving Critical Infrastructure Cybersecurity*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (April 16, 2018), Appendix A, Table 2, *available at* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (last visited on November 19, 2021).

33. NIST guidance includes recommendations for risk assessments, risk management strategies, system access controls, training, data security, network monitoring, breach detection, and mitigation of existing anomalies.[8]

34. CPK's failure to protect massive amounts of PII throughout breach period belies any assertion that CPK employed proper data security protocols or adhered to the spirit of the NIST guidance.

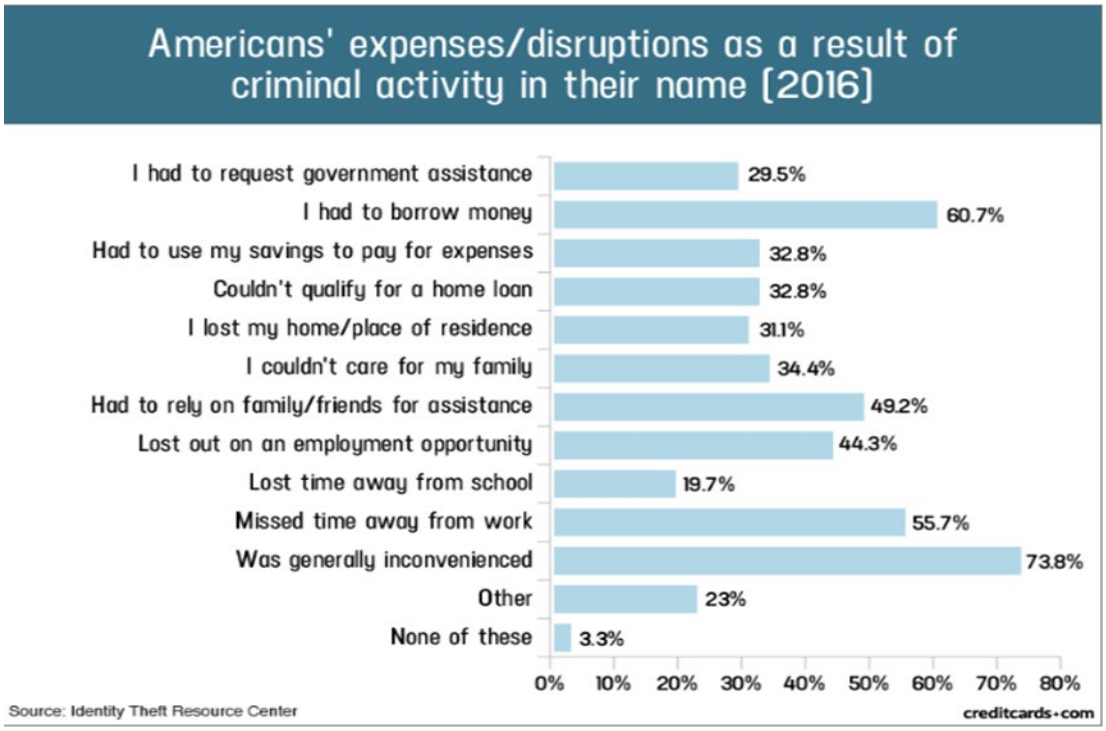
D. Value of Personally Identifiable Information

35. PII is a valuable property right. Its value 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 PII has considerable market value.

36. 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, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[9] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web and that the "*fullz*" (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[10] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[11]

[8] *Id*. at Table 2 pg. 36-43.
[9] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited on November 19, 2021).
[10] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited on November 19, 2021).
[11] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited on November 19, 2021).

37. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of PII.[12]



38. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web.

39. Plaintiffs and the Class have experienced one or more of these harms as a result of the data breach.

40. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and between when PII 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

[12] Source: "*Credit Card and ID Theft Statistics*" by Jason Steele, 10/24/17, https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited on November 19, 2021).

> 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.[13]

41. Therefore, given the importance of safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on its employees as a result of a breach, CPK were, or should have been, fully aware of its responsibilities towards protecting current and former employees' PII.

E. Damage to Plaintiffs and the Class Members Caused by the Data Breach

42. Plaintiffs and the Class Members have been damaged because their PII was accessed by hackers in the Data Breach.

43. Plaintiffs and the Class Members have or will suffer actual injury as a direct result of the Data Breach.

44. As a direct and proximate result of CPK's conduct, Plaintiffs and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud. Plaintiffs now have to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives.

45. On or about November 15, 2021, more than two months after the Data Breach and over a month after discovering the exposure of PII, CPK began notifying current and former employees that their PII may have been compromised. However, the only thing CPK is doing to remedy the harm caused by its breaches is to offer employees a temporary membership to Experian's IdentityWorks.

[13] "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown" by GAO, June 2007, https://www.gao.gov/assets/270/262904.html (last visited on November 19, 2021).

46. Plaintiffs and the Class Members may also incur out-of-pocket costs for protective measures such as credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

47. Plaintiffs and the Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

48. Plaintiffs and the Class have suffered, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. Trespass, damage to and theft of their PII;
b. Improper disclosure of their PII property;
c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by employees' PII being placed in the hands of criminals and misused via the sale of such information on the Internet black market;
d. Damages flowing from CPK's untimely and inadequate notification of the Data Breach;
e. Loss of privacy suffered as a result of the Data Breach;
f. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach; and
g. Ascertainable losses in the form of deprivation of the value of employees' PII for which there is a well-established and quantifiable national and international market.

V. CLASS ALLEGATIONS

49. Plaintiffs bring this action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of themselves and on behalf of all other persons similarly situated ("the Class").

50. Plaintiffs propose the following Class and Sub-Class definitions, subject to amendment as appropriate:

> **Nationwide Class**:
> All individuals in the United States who had any PII compromised as a result of the Data Breach.
> **New York Subclass**:
> All residents of New York who had any PII compromised as a result of the Data Breach.
> **California Subclass**:
> All residents of California who had any PII compromised as a result of the Data Breach.

51. Excluded from each of the above Classes are Defendants and their parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded are any Judge to whom this case is assigned as well as his or her judicial staff and immediate family members.

52. Plaintiffs reserve the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

53. Each of the proposed classes meet the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

54. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class may consist of as many as 100,000 current and former CPK employees whose data was compromised in the Data Breach.

55. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether CPK engaged in the conduct alleged herein;

b. Whether CPK's conduct violated the state consumer protection laws invoked below;

c. When CPK actually learned of the data breach and whether its response was adequate.

d. Whether CPK had a legal duty to adequately protect Plaintiffs' and the Class Members' PII;

e. Whether CPK breached its legal duty by failing to adequately protect Plaintiffs' and the Class Members' PII;

f. Whether CPK had a legal duty to provide timely and accurate notice of the data breach to Plaintiffs and the Class Members;

g. Whether CPK breached its duty to provide timely and accurate notice of the data breach to Plaintiffs and the Class Members;

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

i. Whether CPK knew or should have known that it did not employ reasonable measures to keep Plaintiffs' and the 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 Plaintiffs and the Class Members are entitled to recover actual damages and/or statutory damages;

l. Whether Plaintiffs and the other Class Members are entitled to additional credit or identity monitoring beyond what the company is offering and are entitled to other monetary relief; and

m. Whether Plaintiffs and the Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

56. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PII, like that of every other Class Member, was compromised in the Data Breach.

57. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Class Members. Plaintiffs' Counsel are competent and experienced in litigating class actions, including data breach class actions.

58. Predominance. CPK has engaged in a common course of conduct toward Plaintiffs and the Class Members, in that all the Plaintiffs' and the Class Members' PII was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from CPK's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

59. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact will be superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect

to individual Class Members, which would establish incompatible standards of conduct for CPK. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

60. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2). CPK has acted or has refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

61. Finally, all members of the proposed Classes are readily ascertainable. CPK has access to addresses and other contact information necessary to identify and contact Class Members.

COUNT I

NEGLIGENCE

(On behalf of Plaintiffs and the Nationwide Class)

62. Plaintiffs restate and reallege all proceeding allegations above and hereafter as if fully set forth herein.

63. CPK collected the PII of Plaintiffs and the Nationwide Negligence Class in the course of their employment.

64. CPK knew, or should have known, of the risks inherent in collecting the PII of Plaintiffs and the Class Members and the importance of adequate security. On information and belief, CPK received warnings that hackers routinely attempted to access and acquire PII without authorization. CPK also knew or should have known about numerous, well-publicized data breaches involving other large companies.

65. CPK owed duties of care to Plaintiffs and the Class Members whose PII was entrusted to it. CPK's duties included the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII in its possession;

b. To protect employees' PII using reasonable and adequate security procedures and systems that are compliant with the industry standards;

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, and

d. To promptly notify affected employees of data breaches.

66. By collecting PII data of employees, CPK had a duty of care to use reasonable means to secure and safeguard its computer property, to prevent disclosure of the PII, and to safeguard the PII from theft. CPK's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

67. Because CPK knew that a breach of its systems would damage thousands of its current and former employees, including Plaintiffs and the Class Members, it had a duty to adequately protect their PII.

68. CPK owed a duty of care not to subject Plaintiffs and the Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

69. CPK knew, or should have known, that its systems did not adequately safeguard the PII of Plaintiffs and the Class Members.

70. CPK breached its duties of care by failing to provide, or by acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiffs and the Class Members.

71. CPK breached its duties of care by failing to promptly identify the Data Breach and then provide prompt notice of the Data Breach to Plaintiffs and the Class Members.

72. CPK had a special relationship with Plaintiffs and the Class Members. Plaintiffs' and the Class Members' willingness to entrust CPK with their PII was predicated on the understanding that CPK would take adequate security precautions. Moreover, only CPK had the ability to protect its systems (and the PII that it stored on them) from attack.

73. CPK's own conduct also created a foreseeable risk of harm to Plaintiffs and the Class Members and their PII. CPK's misconduct included failing to:

a. Secure its employee support systems;
b. Secure access to its servers;
c. Comply with industry standard security practices;
d. Employ adequate network segmentation;
e. Implement adequate system and event monitoring;
f. Install updates and patches in a timely manner; and
g. Implement the systems, policies, and procedures necessary to prevent this type of data breach.

74. CPK also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and the Class Members' PII.

75. CPK breached the duties it owed to Plaintiffs and the Class Members in numerous ways, including:

a. By creating a foreseeable risk of harm through the misconduct previously described;
b. By failing to implement adequate security systems, protocols and practices sufficient to protect PII both before and after learning of the data breach;

c. By failing to comply with the minimum industry data security standards during the period of the data breach; and

d. By failing to timely and accurately disclose that the PII of Plaintiffs and the Class Members had been improperly acquired or accessed.

76. But for CPK's wrongful and negligent breach of the duties it owed Plaintiffs and the Class Members, their PII either would not have been compromised or they would have been able to prevent some or all of their damages.

77. As a direct and proximate result of CPK's negligent conduct, Plaintiffs and the Class Members have suffered damages and are at imminent risk of further harm.

78. The injury and harm that Plaintiffs and the Class Members suffered (as alleged above) was reasonably foreseeable.

79. The injury and harm that Plaintiffs and the Class Members suffered (as alleged above) was the direct and proximate result of CPK's negligent conduct.

80. Plaintiffs and the Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II

NEGLIGENCE *PER SE*

(On behalf of Plaintiffs and the Nationwide Class)

81. Plaintiffs restate and reallege all proceeding allegations above and hereafter as if fully set forth herein.

82. Pursuant to Section 5 of the FTCA, 15 U.S.C. § 45, CPK had a duty to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiffs and the Class Members.

83. The FTCA 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.

84. CPK solicited, gathered, and stored PII of Plaintiffs and the Class Members.

85. CPK violated the FTCA by failing to use reasonable measures to protect PII of Plaintiffs and the Class and not complying with applicable industry standards, as described herein.

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

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

88. CPK also violated state laws, as discussed below, and Plaintiffs and the Class are within the class of persons such laws intended to protect.

89. As a direct and proximate result of CPK's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives including, *inter alia*, by closely reviewing and monitoring their accounts for unauthorized activity and other signs of identity theft.

90. CPK breached its duties to Plaintiffs and the Class Members under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and the Class Members' PII.

91. CPK's violation of the FTCA constitutes negligence *per se*.

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

93. The injury and harm suffered by Plaintiffs and the 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 its duties, and that CPK's breach would cause Plaintiffs and the Class Members to experience the foreseeable harms associated with the exposure of their PII.

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

COUNT III

DECLARATORY JUDGMENT

(On behalf of Plaintiffs and the Nationwide Class)

95. Plaintiffs restate and reallege all proceeding allegations above and hereafter as if fully set forth herein.

96. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, 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.

97. CPK owes duties of care to Plaintiffs and the Class Members which required it to adequately secure PII.

98. CPK still possesses Plaintiffs' and the Class Members' PII.

99. Plaintiffs allege that CPK's data security measures remain inadequate. Furthermore, Plaintiffs and the Class Members continue to suffer injury as a result

of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future.

100. Under its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. CPK owes a legal duty to secure Plaintiffs' and the Class Members' PII under the common law and Section 5 of the FTCA;

b. CPK's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect Plaintiffs' and the Class Members' PII;

c. CPK continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII;

d. to comply with its explicit or implicit contractual obligations and duties of care, CPK must implement and maintain reasonable security measures, including, but not limited to:

i. Engaging 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;

ii. Engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. Auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. Segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of CPK's systems;

v. Conducting regular database scanning and securing checks;

vi. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

vii. Meaningfully educating its users about the threats they face as a result of the loss of their PII to third parties, as well as the steps CPK's current and former employees must take to protect themselves.

101. This Court also should issue corresponding prospective injunctive relief requiring CPK to employ adequate security protocols consistent with law and industry standards to protect employees' PII.

102. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at CPK. The risk of another such breach is real, immediate, and substantial. If another breach at CPK occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

103. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to CPK if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to CPK of complying with an injunction by employing reasonable prospective data security

measures is relatively minimal, and CPK has a pre-existing legal obligation to employ such measures.

104. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at CPK, thus eliminating the additional injuries that would result to Plaintiffs and employees whose PII would be further compromised.

COUNT IV

VIOLATION OF THE NEW YORK GENERAL BUSINESS LAW § 349

(On behalf of Plaintiff Kansas Gilleo and the New York Subclass)

105. Plaintiff Gilleo restates and realleges all preceding allegations above and hereafter as if fully set forth herein.

106. New York's General Business Law § 349 ("GBL § 349") prohibits deceptive acts or practices in the conduct of any business, trade, or commerce.

107. In its provision of services throughout the State of New York, CPK conducts business and trade within the meaning and intendment of New York's General Business Law § 349.

108. Plaintiff Gilleo and the New York Subclass Members are persons who have been injured and continue to be injured by CPK's violation of GBL § 349.

109. By the acts and conduct alleged herein, CPK has engaged in deceptive, unfair, and misleading acts and practices, which include, without limitation, the expectation that CPK would implement adequate cybersecurity, when in fact CPK did not.

110. The foregoing deceptive acts and practices were directed at employees.

111. The foregoing deceptive acts and practices are misleading in a material way because they fundamentally misrepresent the ability and measures taken by CPK to safeguard consumer PII, and to induce consumers to enter transactions with CPK.

112. By reason of this conduct, CPK engaged in deceptive conduct in violation of GBL § 349.

113. CPK's actions are the direct, foreseeable, and proximate cause of the damages that Plaintiff Gilleo and the New York Subclass Members have sustained from having provided their PII to CPK, which was exposed in the data breach.

114. As a result of CPK's violations, Plaintiff Gilleo and the New York Subclass Members have suffered damages because: (a) they would not have provided their PII to CPK had they known CPK did not use "reasonable security measures, including physical, administrative, and technical safeguards to help us protect your information from unauthorized access, use and disclosure"; (b) they have suffered identity theft and/or fraudulent charges and their PII has been devalued as a result of being exposed in the data breach; and (c) Plaintiff Gilleo and the New York Subclass Members must spend considerable time and expenses dealing with the effects of the data breach, and are now at greater risk for future harm stemming from the data breach.

115. On behalf of herself and other the New York Subclass Members, Plaintiff Gilleo seeks to recover their actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

COUNT V

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE §§ 17200, *ET SEQ.*

(On behalf of Plaintiff Sydney Rusen and the California Subclass)

116. Plaintiff Sydney Rusen restates and realleges all proceeding allegations above and hereafter as if fully set forth herein.

117. CPK is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

118. CPK violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

119. CPK's unlawful, unfair acts and deceptive acts and practices include:

a. CPK failed to implement and maintain reasonable security measures to protect Plaintiff Rusen and the California Subclass Members from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. CPK failed to:

i. Secure its employee and/or internal website;

ii. Secure access to its servers;

iii. Comply with industry standard security practices;

iv. Employ adequate network segmentation;

v. Implement adequate system and event monitoring;

vi. Install updates and patches in a timely manner, and

vii. Implement the systems, policies, and procedures necessary to prevent this type of data breach.

c. CPK failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff Rusen and the California Subclass Members whose PII has been compromised;

d. CPK's failure to implement and maintain reasonable security measures was 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. These policies are reflected in laws, including 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.*;

e. CPK's failure to implement and maintain reasonable security measures also lead to substantial injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because Plaintiff Rusen and the California Subclass Members could not know of CPK's inadequate security and compromise of its e-commerce site, consumers could not have reasonably avoided the harms that CPK caused;

f. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff Rusen's and the California Subclass Members' PII, including by implementing and maintaining reasonable security measures;

g. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of '' PII, including duties 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.*;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Rusen's and the California Subclass Members' PII;

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Rusen's and the California Subclass Members' PII, including duties 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.*;

j. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82; and

k. Among other ways to be discovered and proved at trial.

120. CPK's representations and omissions to Plaintiff Rusen and the California Subclass Members were material because they were likely to deceive reasonable consumers about the adequacy of CPK's data security and ability to protect the privacy of consumers' PII.

121. CPK intended to mislead Plaintiff Rusen and the California Subclass Members and induce them to rely on its misrepresentations and omissions.

122. Had CPK disclosed to Plaintiff Rusen and the California Subclass Members that its data systems were not secure and, thus, vulnerable to attack, CPK would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, CPK received, maintained, and compiled Plaintiff Rusen's and the California Subclass Members' PII as part of the hiring process without advising Plaintiff Rusen and the California Subclass Members that CPK's data security practices were insufficient to maintain the safety and confidentiality of Plaintiff Rusen and the California Subclass Members. Accordingly, Plaintiff Rusen and the California Subclass Members acted reasonably in relying on CPK's misrepresentations and omissions, the truth of which they could not have discovered.

123. CPK acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff Rusen' and the California Subclass Members' rights.

124. As a direct and proximate result of CPK's unfair, unlawful, and fraudulent acts and practices, Plaintiff Rusen and the California Subclass Members

have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages as described herein and as will be proved at trial.

125. Plaintiff Rusen and the California Subclass Members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from CPK's unfair, unlawful, and fraudulent business practices or use of their PII; declaratory relief; injunctive relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; and other appropriate equitable relief.

126. Plaintiff Rusen and the California Subclass Members are also entitled to injunctive relief requiring CPK to, e.g., (a) strengthen its data security systems and monitoring procedures; (b) submit to future annual audits of those systems and monitoring procedures; and (c) continue to provide adequate credit monitoring to all California Class Members.

COUNT VI

CALIFORNIA CUSTOMER RECORDS ACT ("CCRA")

CAL. CIV. CODE §1798.80, *ET SEQ.*

(On behalf of Plaintiff Sydney Rusen and the California Subclass)

127. Plaintiff Rusen restates and realleges all proceeding allegations above and hereafter as if fully set forth herein.

128. This Count is brought on behalf of Plaintiff Rusen and the California Subclass.

129. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code §1798.81.5, which requires that any 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."

130. CPK is a business that maintains PII about Plaintiff Rusen and the California Subclass Members within the meaning of Cal. Civ. Code §1798.81.5. Such PII includes, but is not limited to, the first and last names of Plaintiff Rusen and the California Subclass and their social security numbers, in addition to other PII. *See* Cal. Civ. Code §1798.81.5(d)(1)(A)(i).

131. Businesses that maintain computerized data that includes PII are 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). Among other requirements, 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.

132. CPK is a business that maintains computerized data that includes PII as defined by Cal. Civ. Code §1798.80.

133. Plaintiff Rusen's and the California Subclass members' PII includes Personal Information as covered by Cal. Civ. Code §1798.82.

134. Because CPK reasonably believed that Plaintiff Rusen and the California Subclass members' PII was acquired by unauthorized persons during the Data Breach, CPK had an obligation to disclose the Data Breach, immediately following its discovery, to the owners or licensees of the PII (i.e., Plaintiff Rusen and the California Subclass) as mandated by Cal. Civ. Code §1798.82.

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

136. As a direct and proximate result of CPK's violations of the Cal. Civ. Code §1798.81.5 and 1798.82, Plaintiff Rusen and the California Subclass members suffered damages, as described above and as will be proven at trial.

137. Plaintiff Rusen and the California Subclass members seek relief under Cal. Civ. Code §1798.84, including actual damages, civil penalties, injunctive relief, and reasonable attorneys' fees and costs.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Classes described above, seek the following relief:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the classes as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representative of the Classes requested herein;

b. Judgment in favor of Plaintiffs and the Class Members awarding them appropriate monetary relief, including actual damages, treble damages, statutory damages, civil penalties, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Classes as requested herein;

d. An order instructing CPK to purchase or provide funds for credit monitoring services for Plaintiffs and all Class Members;

e. An order requiring CPK to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and the Classes awarding them pre-judgment and post judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law, and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

Dated: November 23, 2021

SIRI & GLIMSTAD LLP

By: _____

Mason Barney (*pro hac vice* forthcoming)
Nicholas Armer (Bar No. 330577)
Sonal Jain (*pro hac vice* forthcoming)

Attorneys for Plaintiffs