Daniel O. Herrera (*pro hac vice* anticipated)
Nickolas J. Hagman (*pro hac vice* anticipated)
CAFFERTY CLOBES MERIWETHER
& SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com

Bryan L Clobes (*pro hac vice* anticipated)
CAFFERTY CLOBES MERIWETHER
& SPRENGEL LLP
205 N. Monroe St.
Media, Pennsylvania 19063
Telephone: (215) 864-2800
bclobes@caffertyclobes.com

Roland Tellis (SBN 186269)
rtellis@baronbudd.com
Adam Tamburelli (SBN 301902)
atamburelli@baronbudd.com
BARON & BUDD, P.C.
15910 Ventura Boulevard, Suite 1600
Encino, California 91436
Telephone: (818) 839-2333
Facsimile: (818) 986-9698

Attorneys for Plaintiff and the Putative Class

IN THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
SOUTHERN DIVISION

ESTEBAN MORALES, individually, and on behalf of all others similarly situated,

Plaintiff,

v.

CALIFORNIA PIZZA KITCHEN, INC.,

Defendant.

Case No.:

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

CLASS ACTION COMPLAINT

Plaintiff Esteban Morales ("Plaintiff"), individually, and on behalf of all others similarly situated, by and through his attorneys, brings this action against Defendant California Pizza Kitchen, Inc. ("Defendant" or "CPK"), and alleges as follows based upon personal knowledge as to his own actions, and upon the investigation of counsel regarding all other matters:

I. INTRODUCTION

1. CPK is a chain of restaurants specializing in California-style pizza.[1] CPK owns and operates 270 full-service restaurants in 32 States, numerous smaller locations in airports and stadiums across the United States, and employs tens of thousands of workers, the vast majority of whom are located in the United States. Many of CPK's U.S.-based employees are, like Plaintiff, located in California, where Defendant is headquartered.

2. In order to secure employment with CPK, individuals must provide and entrust Defendant with their most sensitive and valuable resource: their personal information, including names, dates of birth, addresses, and Social Security numbers ("personally identifying information" or "PII").

3. However, despite being a sophisticated business with hundreds of restaurant locations—and employing over the years more than 100,000 individuals who entrusted it with their sensitive and valuable PII—CPK failed to invest in adequate data security and properly safeguard its information systems. As a direct, proximate and foreseeable result of CPK's myriad failures, unauthorized actors compromised the highly-sensitive PII of more than 100,000 current and former employees through an eminently avoidable cybersecurity attack.[2]

---

[1] *Our Company*, California Pizza Kitchen, https://www.cpk.com/about (last accessed Nov. 29, 2021).

[2] *Data Breach Notifications*, Office of the Main Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/ea812f00-c605-4b8e-a6e2-9dd53169b256.shtml (noting that CPK informed the Maine Attorney General's Office that the data breach impacted 103,767 individuals) (last visited Oct. 20, 2021).

4. Specifically, sometime prior to September 15, 2021, Defendant experienced a data breach through which unauthorized individuals accessed and exfiltrated the PII of both current and former CPK employees, including Plaintiff (the "Data Breach"). Critically, many of the categories of PII exposed in the breach, like Social Security numbers, cannot be changed. Yet, Defendant did not disclose the Data Breach to Plaintiff and other affected current and former employees until months after it discovered the Data Breach.

5. CPK's delays virtually ensured that the unauthorized third parties who exploited Defendant's security failure(s) could monetize, misuse and/or disseminate the PII that Defendant allowed to be misappropriated before Plaintiff and others could take affirmative steps to protect their identities. Now, Plaintiff and similarly situated persons will for years suffer the significant and concrete risk that their identities will be (or already have been) stolen and misused.

6. Defendant failed to take adequate and reasonable measures to secure its data systems and all available steps to prevent and stop the Data Breach from occurring; to disclose to current and former employees the material fact that it lacked computer systems and security practices sufficient to safeguard their PII; and to timely detect and provide adequate notice of the Data Breach. Defendant's failures caused substantial harm and injury to Plaintiff and more than 100,000 current and former CPK employees nationwide.

7. As a result of Defendant's negligent, reckless, intentional, and/or unconscionable failure to adequately satisfy its contractual, statutory, and common-law obligations, Plaintiff's and other current and former employees' PII was accessed and acquired by cybercriminals for the express purpose of misusing the data and causing further irreparable harm to CPK's current and former employees' personal, financial, reputational, and future well-being. Plaintiff and other current and former CPK employees face the real, immediate and likely danger of identity theft and the misuse of their PII, especially because their PII was specifically targeted by the hackers.

8. Accordingly, Plaintiff brings this action on behalf of all those similarly situated and against Defendant for its failure to reasonably safeguard Plaintiff's and Class members' PII; failure to reasonably provide timely notification that Plaintiff's and Class members' PII had been accessed and acquired by an unauthorized third party; and for intentionally and unconscionably deceiving Plaintiff and Class members concerning the status, safety, location, access, and protection of their PII.

9. Plaintiff brings claims against Defendant for various statutory violations, as well as negligence, negligence *per se*, breach of implied contract, bailment, and declaratory judgment.

II. PARTIES

A. Plaintiff Morales

10. Plaintiff Esteban Morales ("Plaintiff") is a citizen of California, and currently resides in Bakersfield, California.

11. Plaintiff was employed by CPK at its Bakersfield, California location from 2011 to mid-2016.

12. As a condition of employment, CPK required Plaintiff to: (i) provide CPK with his PII to fulfill CPK's legal responsibilities and operational requirements, including his full name, home address, Social Security number, telephone number(s) and date of birth; and (ii) provide other confidential information in the course of his employment. Plaintiff believes that all CPK employees were required to provide the PII and other confidential information described above as a condition of their employment.

13. Plaintiff accepted CPK's employment offer and provided the above-referenced categories of highly sensitive information prior to commencing and throughout his employment as CPK required, with the expectation that CPK would exercise reasonable care to protect and maintain the confidentiality of his PII and other confidential information by safeguarding it from compromise, disclosure, and misuse by unauthorized users except to the extent necessary to provide agreed-upon compensation

and other employment benefits, and would be timely and forthright relating to any data security incidents involving his PII.

14. In late November 2021, Plaintiff received from CPK a letter dated November 15, 2021, concerning the Data Breach (the "Notice") informing Plaintiff that sometime prior to September 15, 2021, one or more unauthorized persons accessed his PII. Plaintiff was unaware of the breach until he received the November 15 hard copy letter by U.S. Mail.

15. The Notice stated that on October 4, 2021, Defendant determined that Plaintiff's PII, including but not limited to his name and Social Security number were accessed by the unauthorized actor(s).

16. Although Defendant has known of the Data Breach since at least September 15, 2021, Plaintiff did not learn that his PII had been exfiltrated as a direct and foreseeable result of Defendant's failures until he received the Notice more than two months after Defendant discovered the Data Breach. This delay deprived Plaintiff of the opportunity to take affirmative steps to protect his identity before criminals could further abuse and monetize it.

17. The Data Breach already has required Plaintiff to expend significant time and effort to protect himself and his family from its potential adverse consequences, including but not limited to investigating whether hackers have further attempted to misuse his PII, and potential means by which to protect himself from identity theft, such as by placing fraud alerts on his credit accounts at major credit bureaus, reviewing his credit reports, and monitoring associated bank and credit accounts.

18. Because Plaintiff will be at risk of identity theft indefinitely due to the nature of the PII Defendant failed to safeguard, Plaintiff ultimately elected to purchase at an initial annual cost of $167.88, CompleteID, a suite of tools designed to, *inter alia*, protect Plaintiff from identity theft.

19. As a direct, proximate and foreseeable result of the Data Breach, as well as Defendant's failure to prevent against and timely notify Plaintiff of the same, Plaintiff has

suffered concrete injuries and damages, including out-of-pocket costs incurred in mitigating the immediate effects of the Data Breach and the heightened risk of fraud and identity theft to which the Breach exposed him.

20. Plaintiff would not have entrusted his PII to Defendant had Defendant disclosed that it lacked computer systems and data security practices sufficient to adequately safeguard the incredibly sensitive PII of Plaintiff and the Class.

B. Defendant California Pizza Kitchen

21. Defendant California Pizza Kitchen, Inc. ("CPK" or "Defendant") is a Delaware company headquartered at 575 Anton Blvd., Suite 100, Costa Mesa, California 92626.

III. JURISDICTION AND VENUE

22. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because this is a class action in which the matter in controversy exceeds the sum of $5,000,000, the number of class members exceeds 100, and Defendant is a citizen of a State different from that of at least one Class member. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

23. This Court has personal jurisdiction over Defendant because it is authorized to and regularly conducts business in California, and is headquartered in Costa Mesa, California.

24. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a substantial part of the events or omissions giving rise to Plaintiff's and Class members' claims occurred in this District.

IV. GENERAL ALLEGATIONS

A. California Pizza Kitchen, Inc. — Background

25. CPK owns and operates "full-service restaurants" that offer pasta, soup, sandwiches, appetizers, and, CPK's main product and the origin of its name, hearth-baked "California-style" pizzas. In addition to operating more than 270 full-service

restaurants in 38 States, CPK operates smaller locations in airports and stadiums throughout the United States.[3]

26. CPK employs tens of thousands of workers worldwide, most of whom are located in the United States.

27. As a condition of their employment, Defendant required current and former employees to provide it with highly sensitive PII, including but not limited to their: full name, date of birth, address, telephone number, and Social Security number.

28. On information and belief, at the time of the Data Breach CPK stored and maintained the PII of more than 100,000 current and former employees.

29. CPK knows full well the value and importance of data security. CPK's operations routinely involve receiving, storing, processing, and transmitting sensitive information pertaining to its business, customers, and more than 100,000 current and former employees.

30. Current and former employees provided and made their PII available to Defendant with the reasonable expectation that CPK would comply with its obligation to keep their sensitive and personal information, including their PII, confidential and secure from unauthorized access, and that Defendant would provide them with prompt and accurate notice of any unauthorized access to their PII.

31. Unfortunately for Plaintiff and the Class, Defendant failed to carry out its duty to provide adequate data security, and thus failed to protect current and former employees' PII, which unauthorized persons exfiltrated during the Data Breach.

B. The Data Breach

32. According to the Notice that Defendant sent to affected individuals; on or about September 15, 2021, CPK discovered a "disruption to certain systems on [its] computing environment"—the Data Breach.[4]

---

[3] *FAQs*, California Pizza Kitchen, https://www.cpk.com/faqs/general-questions (last accessed Nov. 29, 2021).

[4] *See* Notice, attached hereto as Exhibit 1.

33. Upon discovering the Data Breach, Defendant retained third-party computer forensic specialists and began an investigation of the Data Breach, which led CPK to confirm on or about October 4, 2021, that "certain files on [its] systems" had been accessed by unauthorized individuals. CPK thereafter implemented safeguards it believes would have prevented the Data Breach, including providing additional cybersecurity training for its employees.

34. On or about October 13, 2021, CPK confirmed that files containing sensitive PII belonging to current and former employees were included in the files that were accessed by the unauthorized individuals.

35. CPK has not publicly acknowledged the full extent of PII accessed by unauthorized individuals, but admitted in the Notice it mailed to current and former employees that the PII accessed includes full names and Social Security numbers, and other highly sensitive PII.

36. Additionally, Defendant has not acknowledged the length of time that unauthorized individuals had access to CPK's computer systems, instead stating only that the CPK learned of the "disruption" to its "computer environment" on September 15, 2021. However, based on the type of information accessed and exfiltrated, the unauthorized individuals likely had access to Defendant's computer systems for a significant amount of time prior to September 15, 2021.

37. During the time that the unauthorized individuals had unrestricted access to Defendant's computer systems, they were able to access and acquire personal, sensitive, and protected PII belonging to more than 100,000 current and former employees, including but not limited to their names and Social Security numbers.

C. CPK's Many Failures Both Prior to and Following the Breach

38. Despite learning of the Data Breach on September 15, 2021, and confirming that the sensitive PII of more than 100,000 current and former employees was accessed during the Data Breach on October 13, 2021, Defendant waited until mid-November to

notify current and former employees that CPK had suffered a Data Breach, and that their PII was accessed and extracted by unauthorized persons.

39. Indeed, the Notice letter is dated November 15 and was mailed to and received by current and former employees sometime thereafter. Moreover, when Defendant finally acknowledged that it had experienced a breach, it failed to inform victims the length of time that the individuals had unauthorized access to their PII, or even the full extent of the victims' PII that was accessed during the Data Breach.

40. Defendant, in other words, waited two months after first learning of the Data Breach—and more than a month after determining that highly sensitive PII was accessed—before disclosing the Data Breach to affected individuals.

41. Defendant's failure to properly safeguard Plaintiff's and Class members' PII allowed cybercriminals to access that PII, and its failure to promptly notify Plaintiff and other victims of the Data Breach that their PII had been misappropriated precluded them from taking meaningful steps to safeguard their identities before their PII was disseminated.

42. The Data Breach also demonstrates the inadequacies inherent in Defendant's network monitoring procedures. Had Defendant properly monitored its computer systems, it would have discovered the Data Breach much sooner, and likely long before hackers exfiltrated the PII here at issue.

43. Defendant's lackluster response to the Data Breach only exacerbated the consequences of its IT failings.

44. First, although CPK learned of the Data Breach in September 2021, not until mid-November did it actually notify Plaintiff and the Class that it had allowed their highly-sensitive PII to be accessed. Further, CPK has not admitted to Plaintiff and Class members the full extent of the PII it allowed to be misappropriated, or whether that PII has been made available for purchase (and likely sold) on the dark web.

45. Second, CPK has made no effort to protect Plaintiff and the Class from the long-term consequences of Defendant's acts and omissions. The Notice offered a

complimentary one year membership in Experian IdentityWorks, but because Class members cannot change immutable PII like Social Security numbers, malevolent actors can and will continue to misuse this PII for more than a year. As a result, Plaintiff and the Class will remain at a heightened and unreasonable risk of identity theft for years to come, a risk that a single year of credit monitoring cannot remedy.

46. Indeed, data security experts have stated that the credit monitoring offered by CPK is insufficient to protect victims of the Data Breach.[5]

47. In short, Defendant's myriad failures—including to timely detect the Data Breach and to notify Plaintiff and Class members that their PII had been exfiltrated due to Defendant's security failures—allowed unauthorized individuals to access and misuse Plaintiff's and Class members' PII undetected for months before Defendant finally granted victims the opportunity to take proactive steps to defend themselves and mitigate the near- and long-term consequences of the Data Breach.

D. Data Breaches Pose Significant Threats

48. Data breaches have become a constant threat that, without adequate safeguards, can expose personal data to malicious actors.

49. In 2018, the Identity Theft Resource Center and CyberScout Annual End-of-Year Data Breach Report revealed a 126% increase in exposed data.[6]

50. In fact, Statista, a German entity that collects and markets data relating to, among other things, data breach incidents and the consequences thereof, estimates that the annual number of data breaches occurring in the United States increased by

---

[5] *See* Ty Mezquita, *Employee SSNs Exposed in California Pizza Kitchen Breach*, Business 2 Community (Nov. 28, 2021), https://www.business2community.com/cybersecurity/employee-ssns-exposed-in-california-pizza-kitchen-breach-02443807.

[6] *2018 End of Year Data Breach Report*, Identity Theft Resource Center, available at: https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

approximately 692% between 2005 and 2018, a year during which over 446.5 million personal records were exposed due to data breach incidents.[7] Conditions have only worsened since: Statista estimates that "[i]n 2019, the number of data breaches in the United States amounted to 1,473 with over 164.68 million sensitive records exposed[,]" and that "[i]n the first half of 2020, there were 540 reported data breaches."[8]

51. Securing PII is particularly important in light of the high-profile data breaches that have been reported in recent years, of which a sophisticated entity like CPK knew or should have known, including data breaches at: Arby's, Chipotle, Dairy Queen, Forever 21, GameStop, Harbor Freight Tools, Home Depot, Hy-Vee, Kmart, Lord & Taylor, Michael's Stores, Neiman Marcus, Noodles & Co., P.F. Chang's, Saks Fifth Avenue, Sally Beauty Supply, Schnuck Markets, Sonic Drive-In, SuperValu, Target, T.J. Maxx, Wendy's, Sony, General Electric and many companies.

52. As major companies like Sony, General Electric, Navistar and even the United States government itself have learned, employee records like those misappropriated during the Data Breach make a particularly enticing target. Unlike the records held by retailers and misappropriated through payment system hacks—which consist largely of payment card information that affected individuals can change and thereby protect—employee records offer a treasure trove of immutable PII, such as dates of birth and Social Security numbers, which criminals can use to steal and abuse an individual's identity for years to come.

---

[7] *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2020*, Statista, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-unitedstates-by-number-of-breaches-and-records-exposed (last visited Oct. 20, 2021).

[8] *Id.*

53. Data breaches are a constant threat because of the price that PII fetches on the dark web.[9] According to a recent analysis of data breaches, the average cost of a data breach for a company that employs between 10,000 and 25,000 employees was more than $4.6 million.[10] Another study found that a malicious data breach of employee PII had an average cost of $163 per record accessed.[11]

54. When a data breach occurs, victims must spend significant time, energy, and effort to protect themselves. Cybercriminals use PII to commit identity theft, then engage in fraudulent transactions and obtain consumer credit using the victim's information.

55. Moreover, unlike victims of breaches involving only financial information, victims of data breaches involving sensitive and immutable PII cannot simply "reverse" fraudulent transactions. One study by the Federal Bureau of Investigation found that the average reported loss of employment-related PII was nearly $3,000 per victim.[12]

56. In addition, the Federal Trade Commission ("FTC") has brought dozens of cases against companies that have engaged in unfair or deceptive practices involving inadequate protection of personal data, including recent cases concerning exposure of employee PII against Lookout Services, Inc., Ceridian Corp., and others. The FTC publicized these enforcement actions to place companies, like Defendant, on notice of their obligation to safeguard PII.

---

[9] *See* Brian Stack, *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.

[10] *Cost of a Data Breach Report 2020*, IBM, (July 2020), p.28, available at: https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

[11] *Cost of a Data Breach Report 2020*, IBM, (July 2020), p.20, available at: https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

[12] *Cyber Criminals Use Fake Job Listings to Target Applicants' Personally Identifiable Information*, Federal Bureau of Investigations (Jan. 21, 2020), available at: https://www.ic3.gov/Media/Y2020/PSA200121.

57. The risks identity theft poses can persist indefinitely, and for now and years to come Plaintiff and Class members will suffer the significant and concrete risk that their PII will be (or already has been) misappropriated, and that their identities stolen.

58. Other categories of PII compromised in the Data Breach pose lifelong concerns. While individuals can change credit card numbers or open a new bank account in response to a breach, Plaintiff and the Class cannot change their Social Security or driver's license numbers.

59. Neal O'Farrell, a security and identity theft expert for Credit Sesame, calls a Social Security number "your secret sauce," that is "as good as your DNA to hackers."[13]

60. Unfortunately, Plaintiff and Class members will have to wait until they become victims of Social Security number misuse before they can obtain a new one. But even then, the Social Security Administration warns "that a new number probably won't solve all [] problems . . . and won't guarantee . . . a fresh start." In fact, "[f]or some victims of identity theft, a new number actually creates new problems."[14] One of those new problems is that a new Social Security number will have a completely blank credit history, making it difficult to get credit for years unless it is linked to the old compromised number.

E. CPK had a Duty and Obligation to Protect PII

61. Defendant has an obligation, both statutory and self-imposed, to keep confidential and protect from unauthorized access and/or disclosure Plaintiff's and the Class' PII. Defendant's obligations are derived from: 1) government regulations and state

---

[13] Cameron Huddleston, *How to Protect Your Kids from the Anthem Data Breach*, Kiplinger (Feb. 11, 2015), www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html.

[14] *Identity Theft and Your Social Security Number*, Social Security Admin. (July 2021), at pp. 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf.

laws, and FTC rules and regulations; 2) industry standards; and 3) promises and representations regarding the handling of sensitive PII. Plaintiff and Class members provided, and Defendant obtained, their PII on the understanding that Defendant would protect and keep the PII from unauthorized access or disclosure.

62. The FTC has issued numerous guides for businesses highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-marking.[15]

63. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[16] The guidelines note businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.[17] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[18] Defendant clearly failed to do any of the foregoing, as evidenced by the length of the Data Breach, and the amount of data exfiltrated.

64. Here, at all relevant times, Defendant was fully aware of its obligation to protect the PII of current and former employees, including Plaintiff and the Class,

---

[15] *Start With Security*, Federal Trade Commission (June 2015), available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[16] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (Jan. 23, 2015), available at https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

[17] *Id*.

[18] *Id*.

because it is a sophisticated and technologically savvy business entity that relies extensively on information technology systems and networks, and routinely maintains and transmits PII in order to operate its business.

65. Defendant, as the current and/or former employer of Plaintiff and the Class, had and continues to have a duty to exercise reasonable care in collecting, storing, and protecting the PII of current and former employees from the foreseeable risk of a data breach. The duty arises out of the special relationship that exists between Defendant and its employees, and Defendant's requirement that employees and their family members submit their sensitive, non-public personal information, such as their PII, to Defendant for purposes of employment. Defendant alone had the exclusive ability to implement adequate security measures on its computer systems to secure and protect Plaintiff's and Class members' PII.

66. Defendant also was aware of the significant consequences of its failure to do so because it collected sensitive information, including PII, from thousands of employees annually, and knew that this data, if hacked, would injure current and former employees, including Plaintiff and Class members.

67. Defendant's failure to follow the FTC guidelines and its subsequent failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee data constitute unfair acts or practices prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 14 U.S.C. § 45.

68. Additionally, Defendant had a duty to promptly notify Plaintiff and Class members that their PII was accessed by unauthorized persons, especially when Defendant knew that the highly sensitive and personal information was being sold on the internet.

F. Defendant Violated FTC and Industry Standard Data Protection Protocols

69. The FTC rules, regulations, and guidelines obligate business to protect PII, from unauthorized access or disclosure by unauthorized persons.

70. Unfortunately, Defendant failed to comply with FTC rules, regulations and guidelines, and industry standards concerning the protection and security of PII. As

evidenced by the duration, scope and nature of the Data Breach, among its many deficient practices, Defendant failed in, inter alia, the following respects:

71. Developing and employing adequate intrusion detection systems;

72. Creating effective employee training;

73. Engaging in regular reviews of audit logs and authentication records;

74. Developing and maintaining adequate data security systems to reduce the risk of data breaches and cyberattacks;

75. Ensuring the confidentiality and integrity of current and former employees' PII;

76. Protecting against any reasonably anticipated threats or hazards to the security or integrity of current and former employees' PII;

77. Implementing policies and procedures to prevent, detect, contain, and correct security violations;

78. Developing adequate policies and procedures to regularly review records of system activity, such as audit logs, access reports, and security incident tracking reports;

79. Implementing technical policies, procedures and safeguards for electronically stored information concerning PII that permit access for only those persons or programs that have specifically been granted access; and

80. Other similar measures to protect the security and confidentiality of current and former employees' PII.

81. Had Defendant implemented the above-described data security protocols, policies, and/or procedures, the consequences of the Data Breach could have been avoided or greatly reduced. Defendant could have prevented or detected the Data Breach prior to the hackers accessing Defendant's systems and extracting sensitive and personal information; the amount and/or types of PII accessed by the hackers could have been avoided or greatly reduced; and current and former employees would have been notified sooner, allowing them to promptly take protective and mitigating actions.

G. Defendant's Data Security Practices are Inadequate and Inconsistent with its Self-Imposed Data Security Obligations

82. Defendant purports to care about data security and safeguarding employees' PII, and represents that it will keep secure and confidential the PII that current and former employees provided.

83. Plaintiff and the Class thus entrusted their PII to Defendant in reliance on its promises and self-imposed obligations to keep their PII confidential, and to secure their PII from unauthorized access by malevolent actors. It failed to do so in violation of its own privacy policies.

84. The length of the Data Breach also demonstrates that Defendant failed to safeguard PII by, *inter alia*: maintaining an adequate data security environment to reduce the risk of a data breach; periodically auditing its security systems to discover intrusions like the Data Breach; and retaining outside vendors to periodically test its network, servers, systems and workstations.

85. Had Defendant undertaken the actions that federal and state law require, the Data Breach could have been prevented or the consequences of the Data Breach significantly reduced, as Defendant would have detected the Data Breach prior to the hackers extracting data from Defendant's systems, and current and former employees would have been notified of the Data Breach sooner, allowing them to take necessary protective or mitigating measures much earlier.

86. Indeed, following the Data Breach, Defendant effectively conceded that its security practices were inadequate and ineffective. In the Notice letters it belatedly sent to Plaintiff and others, Defendant acknowledged that the Data Breach required it to implement multiple remedial measures to "reinforce the security of [its] computing environment" and "further protect against similar incidents[,][19] remedial measures that include the above-referenced policies and procedures, which CPK would already have

[19] Notice, Exhibit 1.

had in place had it complied with its legal obligations and followed industry best-practices.

H. Plaintiff and Class Members Suffered Harm Resulting from the Data Breach

87. Like any data hack, the Data Breach presents major problems for all affected. According to Jonathan Bowers, a fraud and data specialist at fraud prevention provider Trustev, "Give a fraudster your comprehensive personal information, they can steal your identity and take out lines of credit that destroy your finances for years to come."[20]

88. The FTC warns the public to pay particular attention to how they keep personally identifying information including Social Security numbers and other sensitive data. As the FTC notes, "[t]hat's what thieves use most often to commit fraud or identity theft." And once they have this information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[21]

89. The ramifications of Defendant's failure to properly secure PII, including Plaintiff's and Class members' PII, are severe. Identity theft occurs when someone uses another person's financial, and personal information, such as that person's name, address, Social Security number, and other information, without permission to commit fraud or other crimes.

90. According to data security experts, one out of every four data breach notification recipients becomes a victim of identity fraud.

91. In response to the Data Breach, Defendant offered to provide certain individuals whose PII was exposed in the Data Breach with one year of credit

---

[20] Roger Cheng, *Data Breach Hits Roughly 15M T-Mobile Customers, Applicants*, CNET (Oct. 1, 2015), available at: http://www.cnet.com/news/data-breach-snags-data-from-15m-t-mobile-customers/.

[21] *What to Know About Identity Theft*, Federal Trade Comm'n (March 2021), available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft.

monitoring. Victims of the Data Breach who were offered the credit monitoring have a small window—only a couple of months from the issuance of the Notice—to receive the written notice and sign up for the credit monitoring.

92. Moreover, the credit monitoring offered by Defendant is inadequate to protect them from the injuries resulting from the unauthorized access and exfiltration of their sensitive PII.

93. Here, due to the Breach, Plaintiff and Class members have been exposed to injuries that include, but are not limited to:

a. Theft of PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of financial accounts as a direct and proximate result of the PII stolen during the Data Breach;

c. Damages arising from the inability to use accounts that may have been compromised during the Data Breach;

d. Costs associated with spending time to address and mitigate the actual and future consequences of the Data Breach, such as finding fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, placing freezes and alerts on their credit reports, contacting their financial institutions to notify them that their personal information was exposed and to dispute fraudulent charges, imposition of withdrawal and purchase limits on compromised accounts, including but not limited to lost productivity and opportunities, time taken from the enjoyment of one's life, and the inconvenience, nuisance, and annoyance of dealing with all issues resulting from the Data Breach, *if* they were fortunate enough to learn of the Data Breach despite Defendant's delay in disseminating notice in accordance with state law;

e. The imminent and impending injury resulting from potential fraud and identity theft posed because their PII is exposed for theft and sale on the dark web; and

f. The loss of Plaintiff's and Class members' privacy.

94. Plaintiff and Class members have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII being accessed by cybercriminals, risks that will not abate within a mere year: the unauthorized access of Plaintiff's and Class members' PII, especially their Social Security numbers, puts Plaintiff and the Class at risk of identity theft indefinitely, and well beyond the limited period of credit monitoring that Defendant offered victims of the Breach. The one year of credit monitoring that Defendant offered to certain victims of the Data Breach is inadequate to mitigate the aforementioned injuries Plaintiff and Class suffered as a result of the Data Breach.

95. As a direct and proximate result of Defendant's acts and omissions in failing to protect and secure current and former employees' PII, Plaintiff and Class members have been placed at a substantial risk of harm in the form of identity theft, and have incurred and will incur actual damages in an attempt to prevent identity theft.

96. Plaintiff retains an interest in ensuring there are no future breaches, in addition to seeking a remedy for the harms suffered as a result of the Data Breach on behalf of both himself and similarly situated individuals whose PII was accessed in the Data Breach.

97. Defendant is aware of the ongoing harm that the Data Breach has and will continue to impose on current and former employees, as the notices that it posted and sent to regarding the Data Breach advise the victims to review their account statements and credit reports for fraudulent or questionable activity.

V. CLASS ALLEGATIONS

98. Plaintiff brings this action on behalf of himself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a Class of:

> All current and former CPK employees whose PII was accessed in the Data Breach.

Excluded from the Class are Defendant, its executives, officers, and the Judge(s) assigned to this case. Plaintiff reserves the right to modify, change or expand the Class definition after conducting discovery.

99. In the alternative, Plaintiff brings this action on behalf of himself and, pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), a subclass of:

> All current and former CPK employees who reside in California whose PII was accessed in the Data Breach (the "California Subclass").

Excluded from the California Subclass are Defendant, its executives, officers, and the Judge(s) assigned to this case.

100. Numerosity: Upon information and belief, the Class is so numerous that joinder of all members is impracticable. While the exact number and identities of individual members of the Class are unknown at this time, such information being in the sole possession of Defendant and obtainable by Plaintiff only through the discovery process, Plaintiff believes, and on that basis alleges, that more than 100,000 individuals comprise the Class and were affected by the Data Breach. Indeed, Defendant admitted that the Data Breach affected more than 100,000 individuals in its notification to the Maine Attorney General's Office. The members of the Class will be identifiable through information and records in Defendant's possession, custody, and control.

101. Existence and Predominance of Common Questions of Fact and Law: Common questions of law and fact exist as to all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to:

a. Whether Defendant's data security and retention policies were unreasonable;

b. Whether Defendant failed to protect the confidential and highly sensitive information with which it was entrusted;

c. Whether Defendant owed a duty to Plaintiff and Class members to safeguard their PII;

d. Whether Defendant breached any legal duties in connection with the Data Breach;

e. Whether Defendant's conduct was intentional, reckless, willful or negligent;

f. Whether an implied contract was created concerning the security of Plaintiff's and Class members' PII;

g. Whether Defendant breached that implied contract by failing to protect and keep secure Plaintiff's and Class members' PII and/or failing to timely and adequately notify Plaintiff and Class members of the Data Breach;

h. Whether Plaintiff and Class members suffered damages as a result of Defendant's conduct; and

i. Whether Plaintiff and Class Members are entitled to monetary damages, injunctive relief and/or other remedies and, if so, the nature of any such relief.

102. Typicality: All of Plaintiff's claims are typical of the claims of the Class since Plaintiff and all members of the Class had their PII compromised in the Data Breach. Plaintiff and the members of the Class sustained damages as a result of Defendant's uniform wrongful conduct.

103. Adequacy: Plaintiff is an adequate representative because his interests do not materially or irreconcilably conflict with the interests of the Class he seeks to represent, he has retained counsel competent and highly experienced in complex class action litigation, and intends to prosecute this action vigorously. Plaintiff and his counsel will fairly and adequately protect the interests of the Class. Neither Plaintiff nor his counsel have any interests that are antagonistic to the interests of other members of the Class.

104. Superiority: A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and members of the Class. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. It would be virtually impossible for members of the Class individually to effectively redress the wrongs done to them. Even if the members of the Class could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and to the court system presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Members of the Class can be readily identified and notified based on, inter alia, Defendant's records and databases.

105. Defendant has acted, and refused to act, on grounds generally applicable to the Class, thereby making appropriate final relief with respect to the Class as a whole.

VI. CAUSES OF ACTION AND CLAIMS FOR RELIEF

COUNT I — Negligence

(By Plaintiff on behalf of the Class, or, in the alternative, the California Subclass)

106. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

107. This count is brought on behalf of all Class members.

108. Defendant owed a duty to Plaintiff and the Class to use and exercise reasonable and due care in obtaining, retaining, and securing the PII that Defendant collected.

109. Defendant owed a duty to Plaintiff and the Class to provide security, consistent with industry standards and requirements, and to ensure that its computer

systems and networks, and the personnel responsible for them, adequately protected the PII that Defendant collected.

110. Defendant owed a duty to Plaintiff and the Class to implement processes to quickly detect a data breach, to timely act on warnings about data breaches, and to inform the victims of a data breach as soon as possible after it is discovered.

111. Defendant owed a duty of care to Plaintiff and the Class because they were a foreseeable and probable victim of any inadequate data security practices.

112. Defendant solicited, gathered, and stored the PII provided by Plaintiff and the Class.

113. Defendant knew or should have known it inadequately safeguarded this information.

114. Defendant knew that a breach of its systems would inflict millions of dollars of damages upon Plaintiff and the Class, and Defendant was therefore charged with a duty to adequately protect this critically sensitive information.

115. Defendant had a special relationship with Plaintiff and the Class. Plaintiff's and Class members' willingness to entrust Defendant with their PII was predicated on the understanding that Defendant would take adequate security precautions. Moreover, only Defendant had the ability to protect its systems and the PII stored on them from attack.

116. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and the Class and their PII. Defendant's misconduct included failing to: (1) secure its systems, servers and workstations, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the safeguards, policies, and procedures necessary to prevent this type of data breach.

117. Defendant breached its duties to Plaintiff and the Class by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII of Plaintiff and Class members.

118. Defendant breached its duties to Plaintiff and Class members by creating a foreseeable risk of harm through the misconduct previously described.

119. Defendant breached the duties it owed to Plaintiff and the Class by failing to implement proper technical systems or security practices that could have prevented the unauthorized access of PII.

120. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PII to Plaintiff and the Class so that Plaintiff and the Class could take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their PII.

121. Defendant breached the duties it owed to Plaintiff and the Class by failing to timely and accurately disclose to Plaintiff and the Class members that their PII had been improperly acquired or accessed.

122. Defendant breached its duty to timely notify Plaintiff and the Class of the Data Breach by failing to provide direct notice to Plaintiff and Class members concerning the Data Breach until (at earliest) November 15, 2021.

123. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered a drastically increased risk of identity theft, relative to both the time period before the breach, as well as to the risk born by the general public, as well as other damages, including but not limited to time and expenses incurred in mitigating the effects of the Data Breach.

124. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and the Class have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II – Negligence *Per Se*

(By Plaintiff on behalf of the Class, or, in the alternative, the California Subclass)

125. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

126. This count is brought on behalf of all Class members.

127. The California Customer Records Act ("CCRA"), Cal. Civ. Code § 1798.80, et seq., requires that entities in possession of PII 1) take reasonable measures to protect the PII, and 2) timely and fully disclose to any breach of the security of the PII in the entity's possession.

128. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies, such as Defendant, of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

129. Defendant violated the CCRA and FTC rules and regulations obligating companies to use reasonable measures to protect PII by failing to comply with applicable industry standards; and by unduly delaying reasonable notice of the actual breach. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, the foreseeable consequences of a Data Breach and the exposure of Plaintiff's and Class members' sensitive PII.

130. Defendant's violations of the CCRA and Section 5 of the FTC Act constitutes negligence per se.

131. Plaintiff and the Class are within the category of persons the CCRA and FTC Act were intended to protect.

132. The harm that occurred as a result of the Data Breach described herein is the type of harm the CCRA and FTC Act were intended to guard against.

133. As a direct and proximate result of Defendant's negligence per se, Plaintiff and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Defendant's possession, and are entitled to damages in an amount to be proven at trial.

COUNT III – Breach of Implied Contract

(By Plaintiff on behalf of the Class, or, in the alternative, the California Subclass)

134. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

135. This count is brought on behalf of all Class members.

136. As a condition of their employment by CPK, Plaintiff and Class members provided Defendant with their PII.

137. By providing their PII, and upon Defendant's acceptance of such information, Plaintiff and Class members, on one hand, and Defendant, on the other hand, entered into implied-in-fact contracts for the provision of data security, separate and apart from any express contract entered into between the parties.

138. The implied contracts between Defendant and Class members obligated Defendant to take reasonable steps to secure, protect, safeguard, and keep confidential Plaintiff's and Class members' PII. The terms of these implied contracts are described in federal laws, state laws, and industry standards, as alleged above. Defendant expressly adopted and assented to these terms in its public statements, representations and promises as described above.

139. The implied contracts for data security also obligated Defendant to provide Plaintiff and Class members with prompt, timely, and sufficient notice of any and all unauthorized access or theft of their PII.

140. Defendant breached the implied contracts by failing to take, develop and implement adequate policies and procedures to safeguard, protect, and secure the PII of Plaintiff and Class members and allowing unauthorized persons to access Plaintiff's and Class members' PII, and failing to provide prompt, timely, and sufficient notice of the Data Breach to Plaintiff and Class members, as alleged above.

141. As a direct and proximate result of Defendant's breaches of the implied contracts, Plaintiff and the Class have been damaged as described herein, will continue to

suffer injuries as detailed above due to the continued risk of exposure of their PII in Defendant's possession, and are entitled to damages in an amount to be proven at trial.

COUNT IV – Bailment

(By Plaintiff on behalf of the Class, or, in the alternative, the California Subclass)

142. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

143. This count is brought on behalf of all Class members.

144. As a requirement of their employment by Defendant, Plaintiff and Class members were provided their PII to Defendant.

145. In delivering their personal information to Defendant, Plaintiff and Class members intended and understood that Defendant would adequately safeguard their PII.

146. Defendant accepted Plaintiff's and Class members' PII.

147. By accepting possession of Plaintiff's and Class members' PII, Defendant understood that Plaintiff and Class members expected Defendant to adequately safeguard their PII. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties.

148. During the bailment (or deposit), Defendant owed a duty to Plaintiff and Class members to exercise reasonable care, diligence and prudence in protecting their PII.

149. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiff's and Class members' PII, resulting in the unlawful and unauthorized access to and misuse of Plaintiff's and Class members' PII.

150. Defendant further breached its duty to safeguard Plaintiff's and Class members' PII by failing to timely notify them that their PII had been compromised as a result of the Data Breach.

151. Defendant failed to return, purge or delete the PII of Plaintiff and members of the Class at the conclusion of the bailment (or deposit) and within the time limits allowed by law.

152. As a direct and proximate result of Defendant's breach of its duties, Plaintiff and Class members suffered consequential damages that were reasonably foreseeable to Defendant, including but not limited to the damages set forth herein.

153. As a direct and proximate result of Defendant's breach of its duty, the PII of Plaintiff and Class members entrusted to Defendant during the bailment (or deposit) was damaged and its value diminished.

COUNT V – Violation of the California Unfair Competition Law

Cal. Bus. & Prof. Code § 17200, *et seq.*

(By Plaintiff on behalf of the Class, or, in the alternative, the California Subclass)

154. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

155. This count is brought on behalf of the Class and California Subclass.

156. The California Unfair Competition Law ("UCL") Cal. Bus. & Prof. Code §17200, et seq., which prohibits, inter alia, "any unlawful, unfair, or fraudulent business act or practice." Cal. Bus. & Prof. Code §17200.

157. Defendant engaged in unlawful, unfair, and fraudulent business acts or practices in violation of the UCL.

158. Defendant's acts, omissions, and conduct were "unlawful" because they violated the FTC Act and were negligent.

159. Defendant's acts, omissions, and conduct were also "unlawful" because they violated the California Customer Records Act ("CCRA"), Cal. Civ. Code § 1798.80, et seq. Defendant failed to take reasonable measures to protect Plaintiff's and Class members' PII, in violation of Cal. Civ. Code § 1798.81.5. Defendant also failed to timely and fully disclose the extent of the Data Breach in the Notice sent to Plaintiff and Class members, in violation of Cal. Civ. Code § 1798.82.

160. Defendant's acts, omissions, and conduct were "unfair" because they offend public policy and constitute immoral, unethical, and unscrupulous activities that caused substantial injury, including to Plaintiff and Class members. The gravity of harm

resulting from Defendant's conduct outweighs any potential benefits attributable to the conduct and there were reasonably available alternatives to further Defendant's legitimate business interests. Defendant's unfair acts and practices include, but are not limited to:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class members' PII, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the industry, which were direct and proximate causes of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class members' PII, including but not limited to duties imposed by the FTC Act, which were direct and proximate causes of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class members' PII, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and the Class members' PII;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class members' PII;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiff's and Class members' PII; and

h. Failing to promptly and adequately notify Plaintiff and Class members that their PII was accessed by unauthorized persons in the Data Breach.

161. Defendant engaged in fraudulent business practices by making material misrepresentations and by failing to disclose material information regarding Defendant's deficient security policies and practices, the security of the PII of Plaintiff and class members, and the Data Breach.

162. Defendant had exclusive knowledge of material information regarding its deficient security policies and practices, and regarding the security of the PII of Plaintiff and Class members. This exclusive knowledge includes, but is not limited to, information that Defendant received through internal and other non-public audits and reviews that concluded that Defendant's security policies were substandard and deficient, and that the PII of Plaintiff and Class members and other CPK data was vulnerable.

163. Defendant also had exclusive knowledge about the extent of the Data Breach, including during the days, weeks, and months following the Data Breach.

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

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

disclose, and actively concealed, information that it had regarding the extent and nature of the Data Breach.

166. Defendant had a duty to disclose the material information that it had because, inter alia, it had exclusive knowledge of the information, it actively concealed the information, it made affirmative statements that were inconsistent with the information it did not disclose, and because Defendant was in a fiduciary position by virtue of the fact that CPK collected and maintained Plaintiff and Class member financial information, medical information, and other PII.

167. Defendant's representations and omissions were material because they were likely to deceive reasonable individuals about the adequacy of Defendant's data security and its ability to protect the confidentiality of current and former employees' PII.

168. Had Defendant disclosed to Plaintiff and Class members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business without adopting reasonable data security measures and complying with the law. Instead, Defendant received, maintained, and compiled Plaintiff's and Class members' PII without advising them that Defendant's data security practices were insufficient to maintain the safety and confidentiality of their PII. Accordingly, Plaintiff and the Class members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

169. Defendant's practices were also contrary to legislatively declared and public policies that seek to protect data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws like the CCRA and FTC Act.

170. The injuries suffered by Plaintiff and Class members greatly outweigh any potential countervailing benefit to consumers or to competition, and are not injuries that Plaintiff and Class members should have reasonably avoided.

171. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiff and Class members as a direct result of Defendant's

unlawful, unfair, and fraudulent acts and practices as set forth in this Complaint include, without limitation:

a. unauthorized charges on their debit and credit card accounts;

b. theft of their PII;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse effects on their credit scores and adverse credit notations;

e. costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate and mitigate the actual and future consequences of the Data Breach, including without limitation finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

f. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. damages to and diminution in value of their personal information entrusted to Defendant for the purpose of employment, and with the understanding that Defendant would safeguard their data against theft and not allow access and misuse of their data by others; and

h. the continued risk to their PII, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect data in its possession.

172. Plaintiff and Class members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendant from disclosing their PII without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

COUNT VI – Violation of State Data Breach Statutes

(By Plaintiff on behalf of the Class, or, in the alternative, the California Subclass)

173. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

174. This count is brought on behalf of all Class members.

175. Defendant is a business that owns, maintains, and licenses PII, and computerized data including PII, about Plaintiff and Class members.

176. Defendant is in possession of PII belonging to Plaintiff and the Class and is responsible for reasonably safeguarding that PII consistent with the requirements of the applicable laws pertaining hereto.

177. Defendant failed to safeguard, maintain, and dispose of, as required, the PII within its possession, custody, or control as discussed herein, which it was required to do by all applicable State laws.

178. Defendant, knowing and/or reasonably believing that Plaintiff's and Class members' PII was acquired by unauthorized persons during the Data Breach, failed to provide reasonable and timely notice of the Data Breach to Plaintiff and the Class as required by following data breach statutes.

179. Defendant's failure to provide timely and accurate notice of the data breach violated the following state data breach statutes:

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

b. Ark. Code Ann. § 4-110-105(a), *et seq.*;

c. Cal. Civ. Code § 1798.80, *et seq.*;

d. Colo. Rev. Stat. Ann § 6-1-716(2), *et seq.*;

e. Conn. Gen. Stat. Ann. § 36a-701b(b), *et seq.*;

f. Del. Code Ann. Tit. 6 § 12B-102(a), *et seq.*;

g. D.C. Code § 28-3852(a), *et seq.*;

h. Fla. Stat. Ann. § 501.171(4), *et seq.*;

i. Ga. Code Ann. § 10-1-912(a), *et seq.*;

j. Haw. Rev. Stat. § 487N-2(a), *et seq.*;

k. Idaho Code Ann. § 28-51-105(1), *et seq.*;

l. Ill. Comp. Stat. Ann. 530/10(a), *et seq.*;

m. Iowa Code Ann. § 715C.2(1), *et seq.*;

n. Kan. Stat. Ann. § 50-7a02(a), *et seq.*;

o. Ky. Rev. Stat. Ann. § 365.732(2), *et seq.*;

p. La. Rev. Stat. Ann. § 51:3074(A), *et seq.*;

q. Md. Code Ann., Commercial Law § 14-3504(b), *et seq.*;

r. Mass. Gen. Laws Ann. Ch. 93H § 3(a), *et seq.*;

s. Mich. Comp. Laws Ann. § 445.72(1), *et seq.*;

t. Minn. Stat. Ann. § 325E.61(1)(a), *et seq.*;

u. Mont. Code Ann. § 30-14-1704(1), *et seq.*;

v. Neb. Rev. Stat. Ann. § 87-803(1), *et seq.*;

w. Nev. Rev. Stat. Ann. § 603A.220(1), *et seq.*;

x. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), *et seq.*;

y. N.J. Stat. Ann. § 56:8-163(a), *et seq.*;

z. N.C. Gen. Stat. Ann. § 75-65(a), *et seq.*;

aa. N.D. Cent. Code Ann. § 51-30-02, *et seq.*;

bb. Okla. Stat. Ann. Tit. 24 § 163(A), *et seq.*;

cc. Or. Rev. Stat. Ann. § 646A.604(1), *et seq.*;

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

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

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

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

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

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

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

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

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

180. As a result of Defendant's failure to reasonably safeguard the Plaintiff's and Class members' PII, and Defendant's failure to provide reasonable and timely notice of the Data Breach to its current and former employees, Plaintiff and the Class have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their PII in Defendant's possession, and are entitled to damages in an amount to be proven at trial.

COUNT VII – Declaratory Judgment

(By Plaintiff on behalf of the Class, or, in the alternative, the California Subclass)

181. Plaintiff incorporates and realleges all allegations above as if fully set forth herein.

182. This count is brought on behalf of all Class members.

183. 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 herein.

184. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard its current and former employees' PII, and whether Defendant is currently

maintaining data security measures adequate to protect Plaintiff and Class members from further data breaches that compromise their PII. Plaintiff alleges that Defendant's data security measures remain inadequate.

185. Plaintiff and 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.

186. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendant continues to owe a legal duty to secure current and former employees' PII, to timely notify current and former employees of any data breach, and to establish and implement data security measures that are adequate to secure current and former employees' PII.

187. The Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect current and former employees' PII.

188. If an injunction is not issued, Plaintiff and Class members will suffer irreparable injury and lack an adequate legal remedy. The threat of another breach of the PII in Defendant's possession, custody, and control is real, immediate, and substantial. If another breach of Defendant's network, systems, servers, or workstations occurs, Plaintiff and Class members will not have an adequate remedy at law, because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

189. The hardship to Plaintiff and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another massive data breach occurs at Defendant, Plaintiff and Class members will likely be subjected to substantial identify theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

190. Issuance of the requested injunction will serve the public interest by preventing another data breach at Defendant, thus eliminating additional injuries to Plaintiff and the tens of thousands of Class members whose confidential information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually, and on behalf of all members of the Class, respectfully requests that the Court enter judgment in their favor and against Defendant, as follows:

A. That the Court certify this action as a class action, proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is a proper class representative; and appoint Plaintiff's Counsel as Class Counsel;

B. That Plaintiff be granted the declaratory relief sought herein;

C. That the Court grant permanent injunctive relief to prohibit Defendant from continuing to engage in the unlawful acts, omissions, and practices described herein;

D. That the Court award Plaintiff and the Class members compensatory, consequential, and general damages in an amount to be determined at trial;

E. That the Court award Plaintiff and the Class members statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

F. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

G. That the Court award pre- and post-judgment interest at the maximum legal rate;

H. That the Court award grant all such equitable relief as it deems proper and just, including, but not limited to, disgorgement and restitution; and

I. That the Court grant all other relief as it deems just and proper.

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the putative Class, demand a trial by jury on all issues so triable.

Dated: December 2, 2021

Respectfully submitted,

/s/ *Roland Tellis*

Roland Tellis (SBN 186269)
rtellis@baronbudd.com
Adam Tamburelli (SBN 301902)
atamburelli@baronbud.com
BARON & BUDD, P.C.
15910 Ventura Boulevard, Suite 1600
Encino, California 91436
Telephone: (818) 839-2333
Facsimile: (818) 986-9698

Daniel O. Herrera (*pro hac vice anticipated*)
Nickolas J. Hagman (*pro hac vice anticipated*)
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
dherrera@caffertyclobes.com
nhagman@caffertyclobes.com

Bryan L Clobes (*pro hac vice anticipated*)
CAFFERTY CLOBES MERIWETHER & SPRENGEL LLP
205 N. Monroe St.
Media, Pennsylvania 19063
Telephone: (215) 864-2800
bclobes@caffertyclobes.com