Kristopher Childers (AZ SBN: 022388)
COMPASSIONATE COUNSEL
3260 N. Hayden Rd., Ste. 210-1
Scottsdale, AZ 85251
P: 602-899-6103
kris@compassionate-counsel.com

Joshua B. Swigart (*pro hac vice forthcoming*)
josh@swigartlawgroup.com
SWIGART LAW GROUP, APC
2221 Camino Del Rio S., Suite 308
San Diego, CA 92108
Tel: (866) 219-3343; Fax: (866) 219-8344

Ben Travis (*pro hac vice forthcoming*)
ben@bentravislaw.com
BEN TRAVIS LAW, APC
4660 La Jolla Village Drive, Suite 100
San Diego, CA 92122
Phone: (619) 353-7966

Attorneys for Plaintiffs Daniel Bozek,
Brandon Gaines and the putative class

UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA

DANIEL BOZEK, an individual; BRANDON GAINES, an individual, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

ARIZONA LABOR FORCE, INCORPORATED; LABOR SYSTEMS, INC.; and DOES 1-10

Defendants.

Case No.:

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

CLASS ACTION

Plaintiffs DANIEL BOZEK ("Bozek") and BRANDON GAINES ("Gaines") (collectively "Plaintiffs"), by and through their attorneys, bring this class action on behalf of themselves, and the Class, as defined below, against Defendants ARIZONA LABOR FORCE, INCORPORATED; LABOR SYSTEMS, INC.; and DOES 1-10 (collectively "Labor Force" or "Defendants"). Plaintiffs hereby allege, on information and belief, except for information based on personal knowledge, which allegations are likely to have evidentiary support after further investigation and discovery, as follows:

INTRODUCTION

1. Plaintiffs brings this Class Action because of Defendants' failure to properly secure and safeguard Plaintiffs' and other similarly situated Labor Force current and former employees' personal information.

2. Defendants operate a staffing agency which employs numerous individuals throughout the country.

3. Plaintiffs and all other persons similarly situated had a right to keep their Personally Identifiable Information ("PII") provided to Defendants confidential (the PII provided to Defendants is collectively referred to as "Sensitive Information"). Plaintiffs and other members of the Class relied on Defendants to keep their Sensitive Information confidential as required by the applicable laws.

4. Defendants violated this right. They failed to implement or follow reasonable data security procedures as required by law and failed to protect Plaintiffs and the proposed Class members' Sensitive Information from unauthorized access.

5. As a result of Defendants' inadequate data security and inadequate or negligent training of their employees, Plaintiffs' and other proposed Class members' Sensitive Information, including their names, addresses, social security numbers and other W-2 information, were made available on the dark web ("Data Breach").

6. Upon information and belief, Defendants have neither notified their employees nor any state attorney general of such breach.

7. The Data Breach was a direct result of Defendants' failure to implement

adequate and reasonable cybersecurity procedures and protocols necessary to protect their employees' Sensitive Information.

8. Defendants disregarded the rights of Plaintiffs and Class members by, among other things, recklessly or negligently failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failing to disclose that they did not have reasonable or adequately robust computer systems and security practices to safeguard their employees' Sensitive Information; failing to take standard and reasonably available steps to prevent the Data Breach; failing to monitor and timely detect the Data Breach; and failing to provide Plaintiffs and Class members prompt and accurate notice of the Data Breach.

9. As a result of Defendants' failure to implement and follow reasonable security procedures, Class members' Sensitive Information is now exposed. Plaintiffs and Class members have spent, and will continue to spend, significant amounts of time and money trying to protect themselves from the adverse ramifications of the Data Breach and dealing with actual fraud and will forever be at a heightened risk of identity theft and fraud.

10. Plaintiffs, on behalf of themselves and all others similarly situated, allege claims for (1) negligence; (2) invasion of privacy; (3) breach of implied contract; (4) breach of fiduciary duty; (5) breach of confidence; (6) violation of the California Unfair Competition Law (Cal. Business & Professions Code § 17200, *et seq*.); (7) violation of the California Customer Records Act ("CCRA") (Cal. Civ. Code § 1798.80, *et seq.*), and (8) violations of the California Consumer Privacy Act ("CCPA") (Cal. Civ. Code § 1798.150, *et seq.*). Plaintiffs and the Class members seek damages, including but not limited to nominal damages from Defendants, and to compel Defendants to adopt reasonably sufficient security practices to safeguard their employees' Sensitive Information that remains in Defendants' custody to prevent incidents like the Data Breach from reoccurring in the future.

JURISDICTION AND VENUE

11. This Court has personal jurisdiction over Defendants because Defendants have conducted and continue to conduct substantial business in this District, have their principal places of business in this District, and have intentionally availed themselves of the laws and markets of Arizona through the operation of their businesses in Arizona.

12. This court has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. 1332(d), as Plaintiffs (California) and Defendants (Arizona, Nevada) are diverse, there are over 100 class members, and the amount in controversy exceeds $5 million.

13. Venue is proper in this Court because Defendants' principal places of business are in this District. Further, a substantial portion of the acts giving rise to this action occurred in this District.

PARTIES

A. PLAINTIFFS

14. Plaintiff Bozek is an individual over the age of eighteen years, and at all times relevant herein was and is, a resident of the County of Orange in the State of California.

15. Plaintiff Gaines is an individual over the age of eighteen years, and at all times relevant herein was and is, a resident of the County of Kern in the State of California.

16. Plaintiffs were formerly employed by Defendants in California. Plaintiffs' Sensitive Information, including their names, addresses, social security numbers and other W-2 information, were taken from Defendants' systems and posted on the dark web.

B. DEFENDANTS

17. Defendant Arizona Labor Force Incorporated is an Arizona corporation with its principal place of business in Arizona.

18. Defendant Labor Systems, Inc. is a Nevada corporation with its principal

place of business in Arizona.

19. Plaintiffs do not know the true names and capacities of defendants sued herein as DOES 1 through 10, and therefore sue these defendants by such fictitious names. Plaintiffs will amend this Complaint to allege the true names and capacities when they are ascertained.

20. Plaintiffs believe and thereon allege that each "Doe" defendant is responsible in some manner for the occurrences herein alleged, and Plaintiffs' injuries and damages as herein alleged are directly, proximately and/or legally caused by such defendant and its acts.

21. Plaintiffs are informed and believe and thereon allege that the aforementioned DOES are somehow responsible for the acts alleged herein as the agents, employers, representatives or employees of the named Defendants, and in doing the acts herein alleged were acting within the scope of their agency, employment or representative capacity of said named Defendants.

FACTUAL ALLEGATIONS

A. Background

22. Defendants operate a staffing agency which employs numerous individuals throughout the country.

23. A common practice for employers, Defendants must keep their employees' Sensitive Information in their systems. Defendants accomplish this by keeping the Sensitive Information electronically—even in their email systems.

24. As employers, Defendants are required to ensure that such sensitive, personal information is not disclosed or disseminated to unauthorized third parties without employees' express, written consent, as further detailed below.

B. The Data Breach

25. Upon information and belief, Defendants' current and former employees' Sensitive Information was recently found on the dark web. Defendants have neither notified the employees nor any state attorney general of such breach. It is unknown

how long such information has been available on the dark web.

26. Defendants failed to put in place proper security protocols to protect against the unauthorized release of employee information and failed to properly train their employees on such protocols, resulting in the unauthorized release of private data. As a result of Defendants' failures, Plaintiffs and the Class members' Sensitive Information was accessed and viewed by unknown and unauthorized third parties and is available on the dark web. This means that the Data Breach was successful: unauthorized individuals accessed Plaintiffs' and the Class members' unencrypted, unredacted information set forth above.

27. Plaintiffs learned that their Sensitive Information, including their names, addresses, social security numbers and other W-2 information, was compromised and is available on the dark web.

28. This kind of Sensitive Information is highly valued by criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200. Social Security numbers are especially valuable to identity thieves.

C. Plaintiffs' Exposure

29. Knowing that thieves stole their Sensitive Information and knowing that their Sensitive Information may now or in the future be available for sale on the dark web has caused Plaintiffs great anxiety. They are now very concerned about fraud and identity theft.

30. Plaintiffs suffered actual injury from having their Sensitive Information exposed as a result of the Data Breach including, but not limited to: (a) damages to and diminution in the value of their Sensitive Information—a form of intangible property that Plaintiffs entrusted to Defendants as a condition for employment; (b) loss of their privacy; (c) imminent and impending injury arising from the increased risk of fraud and identity theft; and (d) the time and expense of mitigation efforts as a result

of the Data Breach.

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

D. Defendants Knew or Should Have Known of the Risk Because Large Employers are Particularly Susceptible to Cyber Attacks.

32. The number of U.S. data breaches surpassed 1,000 in 2016—a record high and a 40 percent increase in the number of data breaches from the previous year.[1] In 2017, 1,579 breaches were reported—a new record high and a 44.7 percent increase in just one year.[2] That trend continues.

33. Defendants knew and understood that unprotected or exposed Sensitive Information in the custody of employers, such as Defendants, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Sensitive Information through unauthorized access. Indeed, when compromised, highly confidential related data is among the most sensitive and personally consequential. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impacts the economy as a whole.

34. As employers, Defendants knew, or should have known, the importance of safeguarding Sensitive Information entrusted to them by Plaintiffs and Class members, and of the foreseeable consequences if their data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class members as a result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent

---

[1] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report from Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), *available at:* https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html (last accessed December 13, 2023).

[2] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review, available at:* https://www.idtheftcenter.org/images/breach/2017Breaches/2017AnnualDataBreachYearEndReview.pdf (last accessed December 13, 2023).

the Data Breach.

E. Defendants Acquire, Collect, and Store Plaintiffs' and Class Members' PII.

35. Defendants acquire, collect, and store a massive amount of their employees' protected confidential information and other personally identifiable data.

36. As a condition of engaging in employment, Defendants require their employees to entrust them with highly confidential Sensitive Information.

37. By requiring, obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class members' Sensitive Information, Defendants assumed legal and equitable duties, and knew or should have known they were responsible for protecting Plaintiffs' and Class members' Sensitive Information from disclosure.

38. Plaintiffs and Class members have taken reasonable steps to maintain the confidentiality of their Sensitive Information. Plaintiffs and Class members relied on Defendants to keep their Sensitive Information confidential and securely maintained, to use this information for business purposes only, to only allow authorized disclosures of this information, and prevent unauthorized disclosure of the information.

F. <u>The Value of PII and the Effects of Unauthorized Disclosure.</u>

39. Defendants were well aware of the highly private nature of the Sensitive Information they collect and its significant value to those who would use it for wrongful purposes.

40. Sensitive Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can commit an array of crimes including identify theft, medical fraud, and financial fraud.[3] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII on multiple underground Internet websites, commonly referred to as the dark web.

41. The ramifications of Defendants' failure to keep Plaintiffs' and Class

[3] Federal Trade Commission, *Warning Signs of Identity Theft, available at:* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last accessed December 13, 2023).

members' Sensitive Information secure are long lasting and severe. Once Sensitive Information is stolen, fraudulent use of that information and damage to victims may continue for years.

42. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding Sensitive Information and of the foreseeable consequences if their data security systems were breached, including the significant costs that would be imposed on their employees as a result of a breach.

G. Defendants Failed to Comply with FTC Guidelines.

43. The Federal Trade Commission ("FTC") promulgates numerous guides for businesses highlighting the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[4]

44. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[5] The guidelines note that businesses should protect the personal customer information 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 any security problems.

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

[4] Federal Trade Commission, *Start With Security*, *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed December 13, 2023).

[5] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed December 13, 2023).

implemented reasonable security measures.[6]

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

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

48. Defendants were at all times fully aware of their obligation to protect Plaintiffs' and Class members' Sensitive Information because of Defendants' position as trusted and experienced employers. Defendants were also aware of the significant repercussions that would result from their failure to do so.

H. Defendants Failed to Comply with Industry Standards.

49. Defendants failed to implement several basic cybersecurity safeguards that can be implemented to improve cyber resilience and require a relatively small financial investment yet can have a major impact on an organization's cybersecurity posture including: (a) the proper encryption of PII; (b) educating and training employees on how to protect PII; and (c) correcting the configuration of software and network devices.

50. Private cybersecurity firms have also identified businesses as being particularly vulnerable to cyber-attacks, both because of the value of the PII they maintain and because employees have been slow to adapt and respond to cybersecurity

[6] FTC, *Start With Security*, *supra*.

threats.[7] These private cybersecurity firms have also promulgated similar best practices for bolstering cybersecurity and protecting against the unauthorized disclosure of PII.

51. Despite the abundance and availability of information regarding the threats and cybersecurity best practices to defend against those threats, Defendants chose to ignore them. These best practices were known, or should have been known by Defendants, whose failure to heed and properly implement industry standards directly led to the Data Breach and the unlawful exposure of Sensitive Information.

I. Plaintiffs and Class Members Suffered Damages.

52. The ramifications of Defendants' failure to keep Plaintiffs' and Class members' Sensitive Information secure are long lasting and severe. Once that kind of Sensitive Information is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.

53. The Sensitive Information belonging to Plaintiffs and Class members is private, sensitive in nature, and left inadequately protected by Defendants—who did not obtain Plaintiffs' or Class members' consent to disclose such Sensitive Information to any other person as required by applicable law and industry standards.

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

[7] Stickman Cyber, *Why Cybersecurity In The Workplace Is Everyone's Responsibility, available at:* https://www.stickmancyber.com/cybersecurity-blog/why-cybersecurity-in-the-workplace-is-everyones-responsibility (last accessed December 13, 2023).

55. Defendants had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite their obligation to protect member data.

56. Defendants could have prevented the intrusions into their systems and, ultimately, the theft of Sensitive Information if Defendants had remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field.

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

58. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems," and that "resolving the problems caused by identity theft may take more than a year for some victims."[8]

59. As a direct result of the Defendants' failures to prevent the Data Breach, Plaintiffs and Class members have suffered, will suffer, and are at increased risk of suffering:

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

b. Out–of–pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended

[8] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013, *available at*: https://www.bjs.gov/content/pub/pdf/vit12.pdf (last accessed December 13, 2023).

and loss of productivity from addressing and attempting to mitigate actual and future consequences of the Data Breach, including but not limited to researching how to prevent, detect, contest, and recover from identity theft and fraud;

d. The continued risk to their Sensitive Information, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect the Sensitive Information in their possession; and

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

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

J. <u>Defendants' Delay in Identifying & Reporting the Breach Caused Additional Harm.</u>

61. It is axiomatic that:

> The quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act.[9]

[9] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, Business Wire, *available at:* https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million (last accessed December 13, 2023).

62. Indeed, once a data breach has occurred:

> [o]ne thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills, insurance invoices, and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them catch cybercriminals and warn other businesses of emerging dangers. If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves (internal citations omitted).[10]

63. Although their Sensitive Information was improperly exposed, Plaintiffs and Class members have still not been notified of the Data Breach, depriving Plaintiffs and Class members of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

64. As a result of Defendants' delay in detecting and notifying consumers of the Data Breach, there is an increased risk of fraud for Plaintiffs and Class members.

CLASS ACTION ALLEGATIONS

65. Plaintiffs bring this class action pursuant to Rule 23(a) and (b)(3) of the Federal Rules of Civil Procedure, on behalf of the following Class and Subclass:

> All individuals whose Sensitive Information stored or possessed by Defendants was subject to the Data Breach (the "Class").
>
> All California residents whose Sensitive Information stored or possessed by Defendants was subject to the Data Breach (the "California Subclass").

[10] Consumer Reports, *The Data Breach Next Door: Security breaches don't just hit giants like Equifax and Marriott. Breaches at small companies put consumers at risk, too*, January 31, 2019, *available at:* https://www.consumerreports.org/data-theft/the-data-breach-next-door/ (last accessed December 13, 2023).

66. Excluded from the Class are Defendants, their officers and directors, families and legal representatives, heirs, successors, or assigns and any entity in which Defendants have a controlling interest, and any Judge assigned to this case and their immediate families.

67. Plaintiffs reserve the right to amend or modify the definition of the Class to provide greater specificity and/or further division into subclasses or limitation to particular issues.

68. **Numerosity:** The members of the Class are so numerous that joinder of all members is impracticable. The exact number or identification of class members is presently unknown, but it is believed that there are thousands of class members in the Class. The identities of the Class Members are ascertainable and can be determined based on records maintained by Defendants.

69. **Predominance of Common Questions:** There are multiple questions of law and fact common to the Class that will predominate over questions affecting only individual class members. The questions of fact and law that are common to the Class members and predominate over questions that may affect individual Class members, include:

a) Whether Plaintiffs' and the Class members' Sensitive Information was accessed and/or viewed by one or more unauthorized persons in the Data Breach alleged above;

b) When and how Defendants should have learned and actually learned of the Data Breach;

c) Whether Defendants' response to the Data Breach was adequate;

d) Whether Defendants owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their Sensitive Information;

e) Whether Defendants breached that duty;

f) Whether Defendants implemented and maintained reasonable security

procedures and practices appropriate to the nature of storing Plaintiffs' and Class members' Sensitive Information;

g) Whether Defendants acted negligently in connection with the monitoring and/or protecting of Plaintiffs' and Class members' Sensitive Information;

h) Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and Class members' Sensitive Information secure and prevent loss or misuse of that Sensitive Information;

i) Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j) Whether Defendants caused Plaintiffs and Class members damages;

k) Whether Defendants violated the law by failing to promptly notify Class members their Sensitive Information was compromised;

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

m) Whether Defendants violated the California Unfair Competition Law (Business & Professions Code § 17200, et seq.);

n) Whether Defendants violated the California Customer Records Act (Cal. Civ. Code § 1798.80, et seq.):

o) Whether Defendants violated the California Consumer Privacy Act ("CCPA") (Cal. Civ. Code § 1798.100, et seq.).

70. **Typicality:** Plaintiffs' claims are typical of those of other Class members because all had their Sensitive Information compromised because of the Data Breach, due to Defendants' virtually identical conduct.

71. **Adequacy:** Plaintiffs are adequate representatives of the Class because they are members of the Class and their interests do not conflict with the interests of the members of the Class they seek to represent. Plaintiffs are represented by

experienced and competent Class Counsel. Class Counsel have litigated numerous class actions. Class counsel intend to prosecute this action vigorously for the benefit of everyone in the Class. Plaintiffs and Class Counsel can fairly and adequately protect the interests of all of the members of the Class.

72. **Superiority:** The class action is superior to other available methods for fairly and efficiently adjudicating this controversy because individual litigation of Class members' claims would be impracticable and individual litigation would be unduly burdensome to the courts. Without the class action vehicle, the Class would have no reasonable remedy and would continue to suffer losses. Further, individual litigation has the potential to result in inconsistent or contradictory judgments. There is no foreseeable difficulty in managing this action as a class action and it provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

First Cause of Action

Negligence

(On Behalf of Plaintiffs and the Class Against all Defendants)

73. Plaintiffs re-allege and incorporate by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

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

75. Defendants had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other

things, designing, maintaining and testing their security protocols to ensure Sensitive Information in Defendants' possession was adequately secured and protected, and that employees tasked with maintaining such information were adequately trained on relevant cybersecurity measures. Defendants also had a duty to put proper procedures in place to prevent the unauthorized dissemination of Plaintiffs' and Class members' Sensitive Information.

76. As a condition of employment, Plaintiffs and Class members were obligated to provide Defendants directly with their Sensitive Information. As such, Plaintiffs and the Class members entrusted their Sensitive Information to Defendants with the understanding that Defendants would safeguard their information.

77. Defendants were in a position to protect against the harm suffered by Plaintiffs and Class members as a result of the Data Breach. However, Plaintiffs and Class members had no ability to protect their Sensitive Information in Defendants' possession.

78. Defendants had full knowledge of the sensitivity of the Sensitive Information, and the types of harm Plaintiffs and Class members could, would, and will suffer if the Sensitive Information were wrongfully disclosed.

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

80. Defendants negligently, through their actions and/or omissions, and unlawfully breached their duty to Plaintiffs and Class members by failing to exercise

reasonable care in protecting and safeguarding Plaintiffs' and Class members' Sensitive Information while the data was within Defendants' possession and/or control by failing to comply with and/or deviating from standard industry rules, regulations, and practices at the time of the Data Breach.

81. The harm the Data Breach caused is the type of harm privacy laws were intended to guard against. And Plaintiffs and Class members are within the class of persons privacy laws were intended to protect.

82. Defendants negligently failed to comply with privacy laws by failing to protect against and prevent the dissemination of Plaintiffs' and Class members' Sensitive Information to unauthorized third parties.

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

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

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

86. The harm the Data Breach caused, and continues to cause, is the type of harm the FTC Act was intended to guard against. The FTC pursues enforcement actions against businesses, which, as a result of their failure to employ reasonable

data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class members.

87. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiffs and Class members by failing to have appropriate procedures in place to detect and prevent unauthorized dissemination of Plaintiffs' and Class members' Sensitive Information.

88. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately disclose to Plaintiffs and Class members the existence and scope of the Data Breach.

89. But for Defendants' wrongful and negligent breach of duties owed to Plaintiffs and Class members, Plaintiffs' and Class members' Sensitive Information would not have been compromised.

90. There is a temporal and close causal connection between Defendants' failure to implement security measures to protect the Sensitive Information and the harm suffered, and/or risk of imminent harm suffered, by Plaintiffs and Class members.

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

92. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiffs and Class members have suffered, and will continue to suffer, the continued risks of exposure of their Sensitive Information, which remains in Defendants'

possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Sensitive Information in their continued possession.

Second Cause of Action

Invasion of Privacy

(On Behalf of Plaintiffs and the Class Against all Defendants)

93. Plaintiffs re-allege and incorporate by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

94. Plaintiffs and Class members had a legitimate expectation of privacy with respect to their Sensitive Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

95. Defendants owed a duty to their members, including Plaintiffs and Class members, to keep their Sensitive Information confidential.

96. The unauthorized release of Sensitive Information, especially social security numbers, is highly offensive to a reasonable person.

97. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class members disclosed their Sensitive Information to Defendants as part of their employment, but privately, with the intention that the Sensitive Information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and Class members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

98. The Data Breach constitutes an intentional interference with Plaintiffs' and Class members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

99. Defendants acted with a knowing state of mind when they permitted the Data Breach because they knew their information security practices were inadequate.

100. Acting with knowledge, Defendants had notice and knew that their inadequate cybersecurity practices would cause injury to Plaintiffs and Class members.

101. As a proximate result of Defendants' acts and omissions, Plaintiffs and Class members' Sensitive Information was disclosed to, and used by, third parties without authorization, causing Plaintiffs and Class members to suffer damages.

102. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class members in that the Sensitive Information maintained by Defendants may be breached again, leading to further viewing, distributing, and use of updated and additional Sensitive Information by unauthorized persons.

103. Plaintiffs and Class members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class members.

Third Cause of Action

Breach of Implied Contract

(On Behalf of Plaintiffs and the Class Against all Defendants)

104. Plaintiffs re-allege and incorporate by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

105. Plaintiffs and Class members were required to provide their Sensitive Information, including their names, social security numbers, addresses, dates of birth, telephone numbers, email addresses, and various other information to Defendants as a condition of employment.

106. Plaintiffs and Class members were paid money by Defendants in exchange for services, along with Defendants' promise to protect their Sensitive Information and other Sensitive Information from unauthorized disclosure.

107. In their written privacy policies, Defendants expressly promised Plaintiffs and Class members that they would only disclose protected information and other

Sensitive Information under certain circumstances, none of which relate to the Data Breach.

108. Defendants promised to comply with privacy standards, and to make sure Plaintiffs' and Class members' Sensitive Information would remain protected.

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

110. Without such implied contracts, Plaintiffs and Class members would not have provided their Sensitive Information to Defendants.

111. Plaintiffs and Class members fully performed their obligations under the implied contract with Defendants. However, Defendants did not.

112. Defendants breached the implied contracts with Plaintiffs and Class members by failing to:

a. Reasonably safeguard and protect Plaintiffs' and Class members' Sensitive Information, which was compromised as a result of the Data Breach; and

b. Identify and respond to suspected or known security incidents.

113. As a direct and proximate result of Defendants' breach of the implied contracts, Plaintiffs and Class members have suffered, and continue to suffer, injuries and damages arising from the Data Breach including, but not limited to: damages from lost time and effort to mitigate the actual and potential impact of the Data

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

Fourth Cause of Action

Breach of Fiduciary Duty

(On Behalf of Plaintiffs and the Class Against all Defendants)

114. Plaintiffs re-allege and incorporate by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

115. In light of their special relationship, Defendants became the guardian of Plaintiffs' and Class members' Sensitive Information. Defendants became fiduciaries, created by their undertaking and guardianship of Plaintiffs' and Class members' Sensitive Information, to act primarily for the benefit of Plaintiffs and Class members. This duty included the obligation to safeguard Plaintiffs' and Class members' Sensitive Information, and to timely notify them in the event of a data breach.

116. Defendants had a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of their relationship. Defendants breached their fiduciary duties owed to Plaintiffs and Class members by failing to:

a. Properly encrypt and otherwise protect the integrity of the system containing Plaintiffs' and Class members' protected confidential information and other Sensitive Information;

b. Timely notify and/or warn Plaintiffs and Class members of the Data Breach; and

c. Otherwise failing to safeguard Plaintiffs' and Class members' Sensitive Information.

117. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiffs and Class members have suffered, and will suffer, injury, including but not limited to: (a) actual identity theft; (b) the loss of the opportunity to control how their Sensitive Information is used; (c) the compromise, publication, and/or theft of their Sensitive Information; (d) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information; (e) lost opportunity costs associated with the effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (f) the continued risk to their Sensitive Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect their employees' Sensitive Information in continued possession; and (g) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Sensitive Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class members.

118. As a direct and proximate result of Defendants' breach of their fiduciary duties, Plaintiffs and Class members have suffered, and will continue to suffer, other forms of injury and/or harm, and other economic and non–economic losses.

Fifth Cause of Action

Breach of Confidence

(On Behalf of Plaintiffs and the Class Against all Defendants)

119. Plaintiffs re-allege and incorporate by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

120. At all times during Plaintiffs' and Class members' interactions with Defendants, Defendants were fully aware of the confidential and sensitive nature of

Plaintiffs' and Class members' Sensitive Information that Plaintiffs and Class members provided to Defendants.

121. As alleged herein and above, Defendants' relationship with Plaintiffs and Class members was governed by terms and expectations that Plaintiffs' and Class members' Sensitive Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

122. Plaintiffs and Class members provided their respective Sensitive Information to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the Sensitive Information to be disseminated to any unauthorized parties.

123. Plaintiffs and Class members also provided their Sensitive Information to Defendants with the explicit and implicit understandings that Defendants would take precautions to protect that Sensitive Information from unauthorized disclosure, such as following basic principles of protecting their networks and data systems, including Defendants' employees' systems.

124. Defendants required and voluntarily received, in confidence, Plaintiffs' and Class members' Sensitive Information with the understanding that the Sensitive Information would not be disclosed or disseminated to the public or any unauthorized third parties.

125. Due to Defendants' failure to prevent, detect, and avoid the Data Breach from occurring by, *inter alia*, following best information security practices to secure Plaintiffs' and Class members' Sensitive Information, Plaintiffs' and Class members' Sensitive Information was disclosed to, and misappropriated by, unauthorized third parties beyond Plaintiffs' and Class members' confidence, and without their express permission.

126. As a direct and proximate result of Defendants' actions and/or omissions, Plaintiffs and Class members have suffered, and will continue to suffer damages.

127. But for Defendants' disclosure of Plaintiffs' and Class members' Sensitive Information in violation of the parties' understanding of confidence, Plaintiffs' and Class members' Sensitive Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants' Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class members' Sensitive Information, as well as the resulting damages.

128. The injury and harm Plaintiffs and Class members suffered, and continue to suffer, was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiffs' and Class members' Sensitive Information. Defendants knew their computer systems and technologies for accepting and securing Plaintiffs' and Class members' Sensitive Information had numerous security and other vulnerabilities placing Plaintiffs' and Class members' Sensitive Information in jeopardy.

129. As a direct and proximate result of Defendants' breaches of confidence, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to: (a) actual identity theft; (b) the compromise, publication, and/or theft of their Sensitive Information; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Sensitive Information; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their Sensitive Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Sensitive Information in their continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class members; and (g) the diminished value of Defendants'

services they received.

130. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non–economic losses.

Sixth Cause of Action

Violation of the California Unfair Competition Law,

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

(On Behalf of Plaintiffs and the California Subclass Against all Defendants)

131. Plaintiffs re-allege and incorporate by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

132. Defendants violated Cal. Bus. & Prof. Code § 17200, *et seq*., by engaging in unlawful, unfair, or fraudulent business acts and practices, that constitute acts of "unfair competition" as defined in Cal. Bus. & Prof. Code § 17200.

133. Defendants engaged in unlawful and unfair acts and practices by establishing the sub–standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and Class members' Sensitive Information with knowledge the information would not be adequately protected; and by storing Plaintiffs' and Class members' Sensitive Information in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendants to take reasonable methods of safeguarding the Sensitive Information of Plaintiffs and Class members.

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

135. As a direct and proximate result of Defendants' unlawful and unfair practices and acts, Plaintiffs and Class members were injured and lost money or property, including but not limited to the loss of Plaintiffs' and Class members'

legally protected interest in the confidentiality and privacy of their Sensitive Information, nominal damages, and additional losses as described herein.

136. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Plaintiffs' and Class members' Sensitive Information and that the risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above–named unlawful practices and acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and Class members.

137. Plaintiffs, on behalf of the Class, seeks relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiff and Class members of money or property Defendants may have acquired by means of Defendants' unlawful, and unfair business practices, restitutionary disgorgement of all monies that accrued to Defendants because of Defendants' unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

Seventh Cause of Action

Violation of the California Customer Records Act ("CCRA")

Cal. Civ. Code § 1798.80, *et seq*.

(On Behalf of Plaintiffs and the California Subclass Against all Defendants)

138. Plaintiffs re-allege and incorporate by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

139. Section 1798.82 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible

and without unreasonable delay."

140. The CCRA further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any 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).)

141. Any person or business required to issue a security breach notification under the CCRA shall meet the following requirements:

a. The security breach notification shall be written in plain language;

b. The security breach notification shall include, at a minimum, the following information:

i. The name and contact information of the reporting person or business subject to this section;

ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

iii. If the information is possible to determine at the time the notice is provided, then any of the following:

1. The date of the breach;

2. The estimated date of the breach; or

3. The date range within which the breach occurred. The notification shall also include the date of the notice.

iv. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

vi. The toll–free telephone numbers and addresses of the major

> credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

142. The Data Breach described herein constituted a "breach of the security system" of Defendants.

143. As alleged above, Defendants unreasonably delayed informing Plaintiffs and Class members about the Data Breach, affecting their Sensitive Information, after Defendants knew the Data Breach had occurred.

144. Defendants failed to disclose to Plaintiffs and Class members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Sensitive Information when Defendants knew or reasonably believed such information had been compromised.

145. Defendants' ongoing business interests gave Defendants incentive to conceal the Data Breach from the public to ensure continued revenue.

146. Upon information and belief, no law enforcement agency instructed Defendants that timely notification to Plaintiffs and Class members would impede their investigation.

147. As a result of Defendants' violation of Cal. Civ. Code § 1798.82, Plaintiffs and Class members were deprived of prompt notice of the Data Breach, and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiff and Class members because their stolen information would have had less value to identity thieves.

148. As a result of Defendants' violation of Cal. Civ. Code § 1798.82, Plaintiffs and Class members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

149. Plaintiffs and Class members seek all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to the damages suffered by Plaintiffs and Class members as alleged above and equitable relief.

Eighth Cause of Action

Violation of the California Consumer Privacy Act ("CCPA")

Cal. Civ. Code § 1798.150, *et seq*.

(On Behalf of Plaintiff and the California Subclass Against all Defendants)

150. Plaintiffs re-allege and incorporate by reference each and every allegation contained in the preceding and subsequent paragraphs as though fully set forth herein.

151. Defendants are corporations organized and operated for profit or financial benefit of their owners with annual gross revenues of more than $25 million. Defendants collect consumers' PII as defined in Cal. Civ. Code § 1798.140.

152. Defendants violated § 1798.150 of the CCPA by failing to prevent Plaintiffs' and Class members' nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

153. Defendants have a duty to implement and maintain reasonable security procedures and practices to protect Plaintiffs' and Class members' PII. As detailed herein, Defendants failed to do so. As a direct and proximate result of Defendants' acts, Plaintiffs' and Class members' PII, including social security numbers, dates of birth and names were subjected to unauthorized access and exfiltration, theft or disclosure.

154. Plaintiffs and Class members seek injunctive or other equitable relief to ensure Defendants hereinafter adequately safeguards employees' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendants continue to hold current and past employees' PII including Plaintiffs' and Class members' PII. Plaintiff and Class members have an

interest in ensuring that their PII is reasonably protected, and Defendants have demonstrated a pattern of failing to adequately safeguard this information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

1. That the Court certify this action as a Class Action under FRCP 23 and appoint Plaintiffs as representatives of the Class and their attorneys as Class Counsel;

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

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

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

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

   iv. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal information of Plaintiffs and Class members' personal information,

   v. prohibiting Defendants from maintaining Plaintiffs' and Class

members' personal information on a cloud-based database,

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

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

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

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

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

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

xii. requiring Defendants to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies,

programs, and systems for protecting personal information,

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

xiv. requiring Defendants to meaningfully educate all Class members about the threats that they face as a result of the loss of their confidential personal information to third parties, as well as the steps affected individuals must take to protect themselves,

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

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

xvii. requiring Defendants to provide ongoing credit monitoring and identity theft repair services to Class members.

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

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

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

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

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury for all claims so triable.

DATED: January 30, 2024

COMPASSIONATE COUNSEL

/s/ Kristopher Childers
Kristopher Childers
Attorneys for Plaintiff

ClassAction.org
