John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive, Penthouse
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Email: jnelson@milberg.com

Attorney for Plaintiff and the Proposed Class

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

SALLY ANDERSEN, individually and on behalf of all others similarly situated, Plaintiff, vs. OAK VIEW GROUP, LLC, Defendant.	Case No. _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Sally Andersen ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendant Oak View Group, LLC ("Oak View" or "Defendant") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises out of the recent cyberattack and data breach ("Data Breach") resulting from Oak View's failure to implement reasonable and industry standard data security practices.

2. Defendant is "the largest developer of sports & live entertainment venues in the world[.]"[1]

3. Plaintiff's and Class Members' sensitive personal information—which they entrusted to Defendant on the mutual understanding that Defendant would protect it against disclosure—was compromised and unlawfully accessed due to the Data Breach.

4. Oak View collected and maintained certain personally identifiable information of Plaintiff and the putative Class Members (defined below), who are (or were) employees at Oak View.

5. The PII compromised in the Data Breach included Plaintiff's and Class Members' full names, dates of birth, and Social Security numbers ("personally identifiable information" or "PII").

6. The PII compromised in the Data Breach was exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals who target PII for its value to identity thieves.

[1] https://www.oakviewgroup.com/

7. As a result of the Data Breach, Plaintiff and approximately 58,000 Class Members,[2] suffered concrete injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) loss of benefit of the bargain; (viii) Plaintiff's PII being disseminated on the dark web, according to Experian; (ix) Plaintiff's credit score being damaged; (x) Plaintiff's experiencing identity theft in the form of an unknown party placing a credit freeze on Plaintiff's account, through Experian; (xi) Plaintiff experiencing a fraudulent charge, for approximately $88, to her US Bank debit card, in or about January 2024; (xii) statutory damages; (xiii) nominal damages; and (xiv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

[2] https://apps.web.maine.gov/online/aeviewer/ME/40/1089d8b9-f2da-42d6-94eb-22e48a9f9cf7.shtml

8. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its employees' PII from a foreseeable and preventable cyber-attack.

9. Defendant maintained the PII in a reckless manner. In particular, the PII was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendant, and thus, Defendant was on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

10. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' PII; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

11. Plaintiff's and Class Members' identities are now at risk because of

Defendant's negligent conduct because the PII that Defendant collected and maintained is now in the hands of data thieves.

12. Armed with the PII accessed in the Data Breach, data thieves have already engaged in identity theft and fraud and can in the future commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

13. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

14. Plaintiff and Class Members may also incur out of pocket costs, *e.g.*, for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

15. Plaintiff brings this class action lawsuit on behalf all those similarly situated to address Defendant's inadequate safeguarding of Class Members' PII that it collected and maintained, and for failing to provide timely and adequate

notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

16. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose PII was accessed during the Data Breach.

17. Plaintiff seeks remedies including, but not limited to, compensatory damages and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

PARTIES

18. Plaintiff, Sally Andersen, is a natural person and resident of Waterloo, Iowa.

19. Defendant is a Delaware limited liability company with its principal place of business located in Los Angeles, California.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are

more than 100 members in the proposed class, and at least one member of the class, including Plaintiff, is a citizen of a state different from Defendant.

21. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, regularly conducts business in California, and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

22. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

FACTUAL ALLEGATIONS

Defendant's Business

23. Defendant is "the largest developer of sports & live entertainment venues in the world[.]"[3]

24. Plaintiff and Class Members are current and former employees at Oak View.

25. As a condition of their employment at Defendant, Plaintiff and Class Members were required to provide their PII to Defendant, including their names, dates of birth, Social Security numbers, and other sensitive information.

26. The information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted PII of Plaintiff and Class Members.

[3] https://www.oakviewgroup.com/

27. Upon information and belief, in the course of collecting PII from employees, Defendant promised to provide confidentiality and adequate security for their data through its applicable privacy notice and through other disclosures in compliance with statutory privacy requirements.

28. Indeed, Defendant provides on its website that: "[w]e have implemented measures designed to protect your Information from accidental loss and from unauthorized access, use, alteration, and disclosure."[4]

29. Plaintiff and Class Members provided their PII to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

30. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiff and Class Members relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

31. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties.

[4] https://www.oakviewgroup.com/privacy-policy/

Defendant has a legal duty to keep employees' PII safe and confidential.

32. Defendant had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

33. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' PII. Without the required submission of PII, Defendant could not perform the services it provides.

34. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

The Data Breach

35. On or about January 8, 2024, Defendant began sending Plaintiff and other Data Breach victims a Notice of Data Security Incident letter (the "Notice Letter"), informing them that:

> What Happened:
>
> On or around November 26, 2023, OVG detected that an unauthorized third party had gained access to parts of its network. Upon detecting the incident, we immediately began executing our established cybersecurity protocols, including proactively taking certain of our systems offline to contain the issue. We also promptly notified the FBI of this incident and engaged industry leading outside cybersecurity experts to assist with securing the network environment and investigating the extent of unauthorized activity.

What Information Was Involved:

OVG has found no evidence that your information has been misused. However, on December 14, 2023, we completed a comprehensive review of the data potentially impacted in this incident and determined that your personal information that may have been impacted included: first name, last name, date of birth, and Social Security number..[5]

36. Omitted from the Notice Letter were the dates of the Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

37. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

38. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

39. The attacker accessed and acquired files Defendant shared with a third

[5] The "Notice Letter". A sample copy is available at https://apps.web.maine.gov/online/aeviewer/ME/40/1089d8b9-f2da-42d6-94eb-22e48a9f9cf7.shtml

party containing unencrypted PII of Plaintiff and Class Members, including their Social Security numbers and other sensitive information. Plaintiff's and Class Members' PII was accessed and stolen in the Data Breach.

40. Plaintiff has already been informed that her PII has been disseminated on the dark web, and Plaintiff further believes that the PII of Class Members was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

Data Breaches Are Preventable

41. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing PII.

42. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

43. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[6]

44. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

[6] *Id.* at 3-4.

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[7]

45. Given that Defendant was storing the PII of its current and former employees, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

46. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of over fifty-eight thousand employees, including that of Plaintiff and Class Members.

[7] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

Defendant Acquires, Collects, And Stores Plaintiff's and the Class's PII

47. Defendant has historically acquired, collected, stored, and shared the PII of Plaintiff and Class Members.

48. As a condition of employment, or as a condition of receiving certain benefits, Defendant requires that its employees and other personnel entrust it with highly sensitive personal information.

49. By obtaining, collecting, sharing, and using Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

50. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

51. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members.

52. Upon information and belief, Defendant made promises to Plaintiff and Class Members to maintain and protect their PII, demonstrating an understanding of the importance of securing PII.

53. Indeed, Defendant provides on its website that: "[w]e have implemented measures designed to protect your Information from accidental loss

and from unauthorized access, use, alteration, and disclosure."[8]

54. Plaintiff and the Class Members relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Defendant Knew or Should Have Known of the Risk Because Employers In Possession Of PII Are Particularly Suspectable To Cyber Attacks

55. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting employers that collect and store PII, like Defendant, preceding the date of the breach.

56. Data breaches, including those perpetrated against employers that store PII in their systems, have become widespread.

57. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[9]

58. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March

[8] https://www.oakviewgroup.com/privacy-policy/

[9] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/

2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the PII that it collected and maintained would be targeted by cybercriminals.

59. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[10]

60. Defendant knew and understood unprotected or exposed PII in the custody of employers, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

61. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

[10] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection

62. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

63. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

64. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen—particularly Social Security numbers—fraudulent use of that information and damage to victims may continue for years.

65. In the Notice Letter, Defendant makes an offer of 12 months of identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

66. Defendant's offer of credit and identity monitoring establishes that Plaintiff's and Class Members' sensitive PII was in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

67. As an employer in custody of its employees' PII, Defendant knew, or should have known, the importance of safeguarding PII entrusted to them by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value Of Personally Identifiable Information

68. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[11]

69. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[12]

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

[11] 17 C.F.R. § 248.201 (2013).
[12] *Id.*

71. Numerous sources cite dark web pricing for stolen identity credentials.[13]

72. For example, PII can be sold at a price ranging from $40 to $200.[14] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[15]

73. PII can sell for as much as $363 per record according to the Infosec Institute.[16] PII is particularly valuable because criminals can use it to target victims with frauds and scams.

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

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

---

[13] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/

[14] *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/

[15] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/

[16] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/

In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

76. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[17] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[18] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

77. Moreover, it is not an easy task to change or cancel a stolen Social Security number:

> An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all

[17] *Identity Theft and Your Social Security Number*, Social Security Administration (2018). Available at https://www.ssa.gov/pubs/EN-05-10064.pdf

[18] *Id*.

> of that old bad information is quickly inherited into the new Social Security number."[19]

78. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

79. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[20]

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

---

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

[20] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf

market."[21]

81. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—names, dates of birth, and Social Security numbers.

Defendant Fails To Comply With FTC Guidelines

82. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight 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.

83. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal employee 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 any security

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

problems.[22]

84. 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.[23]

85. The FTC further recommends that 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 that third-party service providers have implemented reasonable security measures.

86. The FTC has brought enforcement actions against employers for failing to protect employee data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee 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.

---

[22] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

[23] *Id.*

87. These FTC enforcement actions include actions against employers over the compromise of their employees' PII, like Defendant.

88. Defendant failed to properly implement basic data security practices.

89. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

90. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the PII of its employees. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails To Comply With Industry Standards

91. As noted above, experts studying cyber security routinely identify employers in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

92. Several best practices have been identified that, at a minimum, should be implemented by employers in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

93. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

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

95. These foregoing frameworks are existing and applicable industry standards for employers protecting the PII of their employees, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

COMMON INJURIES & DAMAGES

96. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

The Data Breach Increases Victims' Risk Of Identity Theft

97. Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

98. As Plaintiff has already experienced, the unencrypted PII of Class Members will end up for sale on the dark web because that is the *modus operandi*

of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

99. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

100. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

101. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point

for these additional targeted attacks on the victim.

102. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[24]

103. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

104. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a

[24] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/

higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

105. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members.

106. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

107. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss Of Time To Mitigate Risk Of Identity Theft And Fraud

108. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

109. Thus, due to the actual and imminent risk of identity theft, Defendant,

in its Notice Letter, instructs Plaintiff and Class Members to take the following measures to protect themselves: "[r]emain vigilant against attempts at identity theft or fraud, which includes carefully reviewing your accounts for any signs of unauthorized transactions or activity."[25]

110. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, replacing impacted debit cards, contacting financial institutions to sort out fraudulent activity on their accounts, and monitoring their financial accounts for any indication of fraudulent activity, which may take years to detect.

111. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[26]

112. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit

[25] Notice Letter.

[26] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[27]

Diminution Value Of PII

113. PII is a valuable property right.[28] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

114. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[29]

115. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[30,31]

116. Consumers who agree to provide their web browsing history to the

[27] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps
[28] *See, e.g.,* Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[29] https://www.latimes.com/business/story/2019-11-05/column-data-brokers
[30] https://datacoup.com/
[31] https://digi.me/what-is-digime/

Nielsen Corporation can receive up to $50.00 a year.[32]

117. Conversely sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[33]

118. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

119. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change, e.g., names, Social Security numbers, and dates of birth.

120. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false

[32] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

[33] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/

information to police.

121. The fraudulent activity resulting from the Data Breach may not come to light for years.

122. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

123. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to over fifty-eight thousand individuals' detailed personal information, upon information and belief, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

124. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

125. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, the volume of data obtained in the Data Breach, and Plaintiff's PII already being disseminated on the dark web (as discussed below),

there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –*e.g.,* opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

126. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

127. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[34] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

128. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

[34] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1.

129. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

Loss of Benefit of the Bargain

130. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to obtain employment at Defendant under certain terms, Plaintiff and other reasonable employees understood and expected that Defendant would properly safeguard and protect their PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received employment positions of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff Andersen's Experience

131. Plaintiff Sally Andersen is a former employee at Defendant who worked there in or about 2021.

132. As a condition of her employment at Defendant, Plaintiff was required to provide her PII to Defendant, including her names, dates of birth, Social Security numbers, and other sensitive information.

133. Upon information and belief, at the time of the Data Breach,

Defendant retained Plaintiff's PII in its system.

134. Plaintiff Sally Andersen is very careful about sharing her sensitive PII. Plaintiff stores any documents containing her PII in a safe and secure location. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

135. Plaintiff Sally Andersen received the Notice Letter, by U.S. mail, directly from Defendant, dated January 8, 2024. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her name, date of birth, and Social Security number.

136. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, replacing impacted debit cards, contacting financial institutions to sort out fraudulent activity on her accounts, and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

137. Plaintiff suffered actual injury from having her PII compromised as a

result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) loss of benefit of the bargain; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

138. Plaintiff also suffered actual injury in the form of experiencing a fraudulent charge, for approximately $88, to her US Bank debit card, in or about January 2024, which, upon information and belief, was caused by the Data Breach.

139. Plaintiff additionally suffered actual injury in the form of her credit score being damaged, which, upon information and belief, was caused by the Data Breach.

140. Plaintiff further suffered actual injury in the form of an unknown party placing a credit freeze on her account, through Experian, which, upon information and belief, was caused by the Data Breach.

141. Plaintiff further suffered actual injury in the form of her PII being

disseminated on the dark web, according to Experian, which, upon information and belief, was caused by the Data Breach.

142. Plaintiff further suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

143. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

144. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

145. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

146. Plaintiff Sally Andersen has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

147. This action is properly maintainable as a class action. Plaintiff brings this class action on behalf of herself and on behalf of all others similarly situated.

148. Plaintiff proposes the following Class definition, subject to amendment

as appropriate:

> **Nationwide Class**
> All individuals residing in the United States whose PII was compromised in the data breach announced by Defendant in January 2024 (the "Class").

149. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

150. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. At least 58,000 individuals were notified by Defendant of the Data Breach, according to the breach report submitted to Office of the Maine Attorney General.[35] The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

151. Common questions of law and fact exist as to all members of the Class that predominate over any questions affecting solely individual members of the Class. The questions of law and fact common to the Class, which may affect

[35] https://apps.web.maine.gov/online/aeviewer/ME/40/1089d8b9-f2da-42d6-94eb-22e48a9f9cf7.shtml

individual Class members, include, but are not limited to, the following:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g.. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiff and Class Members are entitled to actual damages,

statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct; and

k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

152. Typicality: Plaintiff's claims are typical of those of the other members of the Class because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

153. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Nationwide Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

154. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that

would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action and data breach litigation, and Plaintiff intends to prosecute this action vigorously.

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

156. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable

advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

157. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

158. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

159. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

160. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding

declaratory relief with regard to the Class Members as a whole is appropriate under Code of Civil Procedure § 382.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

161. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein

162. Defendant requires its employees, including Plaintiff and Class Members, to submit non-public PII in the ordinary course of providing its services.

163. Defendant gathered and stored the PII of Plaintiff and Class Members as part of its business of soliciting its services to its employees, which solicitations and services affect commerce.

164. Plaintiff and Class Members entrusted Defendant with their PII with the understanding that Defendant would safeguard their information.

165. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

166. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

167. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

168. Section 5 of the FTC Act, as interpreted and enforced by the FTC, prohibits the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the members of the Class's sensitive PII.

169. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the PII.

170. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of obtaining employment at Defendant.

171. Defendant's duty to use reasonable care in protecting confidential data

arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

172. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

173. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former employees' PII it was no longer required to retain pursuant to regulations.

174. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

175. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

176. Defendant breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures

to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Class Members' PII;

d. Failing to detect in a timely manner that Class Members' PII had been compromised;

e. Failing to remove former employees' PII it was no longer required to retain pursuant to regulations,

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

177. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

178. Defendant's violation of Section 5 of the FTC Act constitutes

negligence.

179. Plaintiff and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm the statute was intended to guard against.

180. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

181. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

182. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches targeting employers in possession of PII.

183. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

184. Plaintiff and the Class were the foreseeable and probable victims of any

inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

185. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

186. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

187. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

188. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

189. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

190. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

191. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

192. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) loss of benefit of the bargain; (viii) Plaintiff's PII being disseminated on the dark web, according to Experian; (ix) Plaintiff's credit score being damaged; (x) Plaintiff's experiencing identity theft in the form of an unknown party placing a credit freeze on Plaintiff's account, through Experian; (xi) Plaintiff experiencing a fraudulent charge, for approximately $88, to

her US Bank debit card, in or about January 2024; (xii) statutory damages; (xiii) nominal damages; and (xiv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

193. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

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

195. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

196. Defendant's negligent conduct is ongoing, in that it still holds the PII of Plaintiff and Class Members in an unsafe and insecure manner.

197. Plaintiff and Class Members are also entitled to injunctive relief

requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

198. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

199. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of their employment at Defendant.

200. Plaintiff and the Class entrusted their PII to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

201. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

202. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business

purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

203. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

204. Defendant solicited, offered, and invited Plaintiff and Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

205. In accepting the PII of Plaintiff and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the PII from unauthorized access or disclosure.

206. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

207. On information and belief, Defendant further promised to comply with

industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

208. Plaintiff and Class Members provided their labor and PII to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

209. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

210. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

211. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

212. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

213. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, as alleged herein,

including the loss of the benefit of the bargain.

214. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

215. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members

COUNT III
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

216. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

217. Plaintiff and Class Members had a legitimate expectation of privacy to their PII and were entitled to the protection of this information against disclosure to unauthorized third parties.

218. Defendant owed a duty to Plaintiff and Class Members to keep their PII confidential.

219. Defendant failed to protect and released to unknown and unauthorized third parties the non-redacted and non-encrypted PII of Plaintiff and Class Members.

220. Defendant allowed unauthorized and unknown third parties access to

and examination of the PII of Plaintiff and Class Members, by way of Defendant's failure to protect the PII.

221. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII of Plaintiff and Class Members is highly offensive to a reasonable person.

222. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and Class Members disclosed their PII to Defendant as a necessary condition of their employment at Defendant, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

223. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's 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.

224. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

225. Because Defendant acted with this knowing state of mind, it had notice

and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

226. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and Class Members was disclosed to third parties without authorization, causing Plaintiff and Class Members to suffer damages.

227. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff 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.

COUNT IV
UNJUST ENRICHMENT / QUASI CONTRACT
(On Behalf of Plaintiff and the Class)

228. Plaintiff restates and realleges the preceding factual allegations set forth above as if fully alleged herein.

229. Plaintiff brings this claim in the alternative to the breach of implied contract claim above.

230. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of providing their valuable PII and/or labor to Defendant.

231. Plaintiff and Class Members provided Defendant their PII on the understanding that Defendant would pay for the administrative costs of reasonable data privacy and security practices and procedures from the revenue it derived therefrom. In exchange, Plaintiff and Class Members should have received adequate protection and data security for such PII held by Defendant.

232. Defendant benefited from receiving Plaintiff's and Class Members' labor and from receiving their PII through its ability to retain and use that information for its own benefit. Defendant understood and accepted this benefit.

233. Defendant knew Plaintiff and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the PII of Plaintiff and Class Members for business purposes.

234. Because all PII provided by Plaintiff and Class Members was similarly at risk from a foreseeable and targeted data breach, Defendant's obligation to safeguard the PII it collected from its employees was inherent to the relationship.

235. Defendant also understood and appreciated that Plaintiff's and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

236. Defendant failed to provide reasonable security, safeguards, and protections to the PII of Plaintiff and Class Members.

237. Defendant enriched itself by saving the costs it reasonably should have

expended on data security measures to secure Plaintiff's and Class Members' PII.

238. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead made calculated decisions to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

239. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

240. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

241. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

242. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

243. Plaintiff and Class Members have no adequate remedy at law.

244. As a direct and proximate result of Defendant's conduct, Plaintiff and

Class Members have suffered and will suffer injury including, but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) experiencing an increase in spam calls, texts, and/or emails; (vii) loss of benefit of the bargain; (viii) Plaintiff's PII being disseminated on the dark web, according to Experian; (ix) Plaintiff's credit score being damaged; (x) Plaintiff's experiencing identity theft in the form of an unknown party placing a credit freeze on Plaintiff's account, through Experian; (xi) Plaintiff experiencing a fraudulent charge, for approximately $88, to her US Bank debit card, in or about January 2024; (xii) statutory damages; (xiii) nominal damages; and (xiv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

245. Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

COUNT V
Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code §17200 *et seq.*
(On Behalf of Plaintiff and the Class)

246. Plaintiff re-alleges and incorporates by reference each and every allegation in this Complaint, as if fully set forth herein.

247. Defendant is a "person" defined by Cal. Bus. & Prof. Code § 17201.

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

249. Defendant's "unfair" acts and practices include:

a. Defendant failed to implement and maintain reasonable security measures to protect Plaintiff's and Class Members' personal information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Defendant Data Breach. Defendant failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

b. Defendant's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected

in laws, including the FTC Act (15 U.S.C. § 45), California's Customer Records Act (Cal. Civ. Code § 1798.80 *et seq.*), and California's Consumer Privacy Act (Cal. Civ. Code § 1798.150);

c. Defendant's failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant's inadequate security, consumers could not have reasonably avoided the harms that Defendant caused; and

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

250. Defendant has engaged in "unlawful" business practices by violating multiple laws, including the FTC Act, 15 U.S.C. § 45, and California common law.

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

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

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, which was a direct and proximate

cause of the Defendant Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Defendant Data Breach;

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

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

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

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

252. Defendant's representations and omissions were material because they

were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' personal information.

253. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiff and Class Members' were injured and lost money or property, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personal information.

254. Defendant's violations were, and are, willful, deceptive, unfair, and unconscionable.

255. Plaintiff and Class Members have lost money and property as a result of Defendant's conduct in violation of the UCL, as stated herein and above.

256. By deceptively storing, collecting, and disclosing their personal information, Defendant has taken money or property from Plaintiff and Class Members.

257. Defendant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and Class Members' rights.

258. Plaintiff and Class Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendant's

unfair, unlawful, and fraudulent business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

D. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the

interests of Plaintiff and Class Members, including but not limited to an order:

i. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

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

iii. Requiring Defendant to delete, destroy, and purge the PII of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. Requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. Prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;

vi. Requiring Defendant 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 Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. Requiring Defendant to conduct regular database scanning and securing checks;

xi. Requiring Defendant 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 identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. Requiring Defendant 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;

xiii. Requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether

monitoring tools are appropriately configured, tested, and updated;

xv. Requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

F. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: January 26, 2024

Respectfully submitted,

s/ John J. Nelson

John J. Nelson (SBN 317598)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
280 S. Beverly Drive, Penthouse
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Fax: (858) 209-6941
Email: jnelson@milberg.com

Attorney for Plaintiff and the Proposed Class

ClassAction.org