UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

ANDREW SMITH and MACKENZIE FAIRFIELD, individually and on behalf of all others similarly situated, Plaintiffs, vs. ACUITY BRANDS, INC., Defendant.	Case No. _____ CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Andrew Smith and Mackenzie Fairfield ("Plaintiffs") bring this Class Action Complaint ("Complaint") against Defendant Acuity Brands, Inc. ("Acuity" or "Defendant") as individuals and on behalf of all others similarly situated, and alleges, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

JURISDICTION AND VENUE

1. 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 Plaintiffs Smith and Fairfield, is a citizen of a state different from Defendant.

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

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

NATURE OF THE ACTION

4. This class action arises out of the recent data breach ("Data Breach") involving Defendant, a "leading industrial technology company" based in Georgia.[1]

5. Plaintiffs bring this Complaint against Defendant for its failure to properly secure and safeguard the personally identifiable information that it collected and maintained as part of its regular business practices, including, but not limited to, names, Social Security numbers, driver's license numbers, financial account numbers, (collectively defined herein as "PII"), and information related to employees' healthcare benefits.

[1] https://www.acuitybrands.com/who-we-are

6. Upon information and belief, current and former Acuity employees are required to entrust Defendant with sensitive, non-public PII, without which Defendant could not perform its regular business activities, in order to obtain employment or certain employment benefits at Defendant. Defendant retains this information for at least many years and even after the employee-employer relationship has ended.

7. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

8. On December 7, 2021, Defendant became aware of suspicious activity on its networks. Defendant proceeded to investigate the nature and scope of the suspicious activity and subsequently concluded that "an unauthorized person obtained access to some of Acuity's systems on December 7 and December 8, 2021, and copied a subset of files out of its network during that time."[2]

9. As a further result of investigation into the Data Breach detected on December 7, 2021, Acuity also uncovered "an unrelated incident of unauthorized

[2] The "*Notice Letter*". Available at https://www.acuitybrands.com/-/media/abl/acuitybrands/files/data-security-incident-notice.pdf?forceBehavior=open

access that occurred on October 6 and October 7, 2020, which included an attempt to copy certain files out of its network."[3]

10. According to Defendant's Notice of Data Security Incident letter (the "Notice Letter"), the compromised PII included individuals' names, Social Security numbers, driver's license numbers, financial account numbers, and information related to employees' healthcare benefits.[4]

11. Defendant's investigation concluded that the PII compromised in the Data Breach included Plaintiffs' and approximately 37,000 other individuals' information.[5]

12. Defendant failed to adequately protect Plaintiffs' and Class Members PII—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted PII was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect customers' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' PII because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

---

[3] *Id.*
[4] *Id.*
[5] https://apps.web.maine.gov/online/aeviewer/ME/40/1af8a682-861a-4e94-a005-d50740ab143f.shtml

13. Moreover, after learning of the Data Breach, Defendant waited *nearly an entire year* (from December 7, 2021, to December 5, 2022) to notify Plaintiffs and Class Members of the Data Breach and/or inform them that their PII was compromised. During this time, Plaintiffs and Class Members were unaware that their sensitive PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

14. In breaching its duties to properly safeguard Plaintiffs' and Class Members' PII and give timely, adequate notice of the Data Breach's occurrence, Defendant's conduct amounts to negligence and/or recklessness and violates federal and state statutes.

15. Plaintiffs brings this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

16. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain

adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

17. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) 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) remain 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.

18. Plaintiffs and Class Members seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated

persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

PARTIES

19. Plaintiff Andrew Smith is and has been, at all relevant times, a resident and citizen of Illinois, currently residing in Dixon, Illinois. Mr. Smith received the Notice Letter, via U.S. mail, directly from Defendant, dated December 5, 2022.

20. Mr. Smith provided his PII to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect his PII. If Mr. Smith had known that Defendant would not adequately protect his PII, he would not have entrusted Defendant with his PII or allowed Defendant to maintain this sensitive PII.

21. Plaintiff Mackenzie Fairfield is and has been, at all relevant times, a resident and citizen of Indiana, currently residing in Crawfordsville, Indiana. Ms. Fairfield received the Notice Letter, via U.S. mail, directly from Defendant, dated December 5, 2022.

22. Ms. Fairfield provided her PII to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect her PII. If Ms. Fairfield had known that Defendant would not adequately protect her PII, she would not have entrusted Defendant with her PII or allowed Defendant to maintain this sensitive PII.

23. Defendant Acuity Brands, Inc. is an industrial lighting and building management solutions provider, incorporated under the laws of the state of Delaware, with its principal office located at 1170 Peachtree Street N.E., Suite 2300, Atlanta, GA, 30309.

24. Acuity Brands, Inc. ("Acuity Brands") is the parent company of Acuity Brands Lighting, Inc. ("ABL") and other subsidiaries (Acuity Brands, ABL, and such other subsidiaries are collectively referred to herein as the "Company"). The Company is one of the world's leading providers of lighting and building management solutions and services for commercial, institutional, industrial, infrastructure, and residential applications throughout North America and select international markets.[6]

DEFENDANT'S BUSINESS

25. Defendant is a Georgia-based company that sells industrial lighting and other products to consumers. Defendant currently employs "over 13,000 associates across 7 countries".[7]

26. Plaintiffs and Class Members are current and former employees at Defendant.

[6] https://www.sec.gov/Archives/edgar/data/1144215/000114421518000110/ayi-20180831x10k.htm
[7] https://www.acuitybrands.com/who-we-are

27. In order to apply to be an employee or obtain certain employment-related benefits at Defendant, Plaintiffs and Class Members were required to provide sensitive and confidential PII, including their names, dates of birth, Social Security numbers, driver's license numbers, financial information, and other sensitive information.

28. The information held by Defendant in its computer systems included the unencrypted PII of Plaintiffs and Class Members.

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

30. Indeed, Defendant's Privacy Statement provides that: "Acuity Brands will take commercially and technologically reasonable precautions to protect your information while it is in our possession."[8]

31. Plaintiffs 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.

[8] https://www.acuitybrands.com/privacy-statement

32. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII. Plaintiffs 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. Plaintiffs and Class Members value the confidentiality of their PII and demand security to safeguard their PII.

33. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumer's PII safe and confidential.

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

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

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

THE DATA BREACH

37. On or about December 5, 2022, Defendant began sending Plaintiffs and other victims of the Data Breach a Notice of Data Event letter, informing them that:

> On December 7, 2021, we identified a data security incident, immediately took steps to secure our systems, and worked with a third-party cybersecurity firm to conduct a thorough investigation. Our investigation determined that an unauthorized person obtained access to some of our systems on December 7 and December 8, 2021, and copied a subset of files out of our network during that time. During our investigation, we also discovered evidence of an unrelated incident of unauthorized access that occurred on October 6 and October 7, 2020, which also included copying certain files out of our network. We conducted a review of our files copied from our network in December 2021 and October 2020. Our review identified that they contained your personal information.[9]

38. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, why it took over nearly a *full year* to inform impacted individuals after Defendant determined their information was involved, why Defendant did not detect the October 2020 data breach on its network prior to investigating the December 2021 Data Breach, 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 Plaintiffs and Class Members, who retain a vested interest in ensuring that their PII remains protected.

[9] Notice Letter.

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

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

41. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted PII of Plaintiffs and Class Members, including their names, Social Security numbers, driver's license numbers, and financial account information. Plaintiffs' and Class Members' PII was accessed and stolen in the Data Breach.

42. Plaintiffs further believe their PII, and that 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

43. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[10]

44. 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, employees and 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

[10] *See* How to Protect Your Networks from RANSOMWARE, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Aug. 23, 2021).

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.[11]

45. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

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

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[12]

[12] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at:* https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Oct. 17, 2022).

46. 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;

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].[13]

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

48. 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 37,000 current and former employees, including that of Plaintiffs and Class Members.

DEFENDANT ACQUIRES, COLLECTS, AND STORES PLAINTIFFS' PII

49. As a condition of employment with Defendant, Plaintiffs and Class Members were required to give their sensitive and confidential PII to Defendant.

50. Defendant retains and stores this information and derives a substantial economic benefit from the PII that it collects. But for the collection of Plaintiffs' and Class Members' PII, Defendant would be unable to perform its business services.

51. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the PII from disclosure.

[13] *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/ (last visited Nov. 11, 2021).

52. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

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

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

55. Indeed, Defendant's Privacy Policy provides that: "Acuity Brands will take commercially and technologically reasonable precautions to protect your information while it is in our possession."[14]

DEFENDANT KNEW, OR SHOULD HAVE KNOWN, OF THE RISK SINCE EMPLOYERS IN POSSESSION OF PII ARE SUSCEPTIBLE TO CYBER ATTACKS

56. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they custody. Defendant knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

[14] https://www.acuitybrands.com/privacy-statement

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

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

59. Additionally, as companies became more dependent on computer systems to run their business,[15] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[16]

[15] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html
[16] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022

60. As a custodian of PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiffs and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

61. Indeed, Defendant's Privacy Statement evidences its knowledge of the foreseeable risks of Data Breaches, like the one it experienced, stating that: "due to the nature of the Internet and current technology, no computer system is completely safe, and we cannot guarantee the security of your information."[17]

62. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[18]

63. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[19]

[17] https://www.acuitybrands.com/privacy-statement
[18] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.
[19] *Id*.

64. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

65. 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."[20]

66. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs 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 Plaintiffs and Class Members as a result of a breach.

67. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially

[20]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 (last accessed Oct. 17, 2022).

thousands of individuals' detailed, PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

68. In the Notice Letter, Defendant makes an offer of 12 months of identity monitoring services. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' PII. Moreover, once this service expires, Plaintiffs and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

69. Defendant's offering of credit and identity monitoring establishes that Plaintiffs and Class Members' sensitive PII *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

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

71. The ramifications of Defendant's failure to keep secure the PII of Plaintiffs 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.

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

VALUE OF PERSONALLY IDENTIFYING INFORMATION

73. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[21] 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."[22]

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

[21] 17 C.F.R. § 248.201 (2013).
[22] *Id.*

pricing for stolen identity credentials.[23] For example, Personal Information can be sold at a price ranging from $40 to $200.[24] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[25]

75. Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiffs and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[26]

---

[23] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Oct. 17, 2022).

[24] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 17, 2022).

[25] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 217, 2022).

[26] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Oct. 17, 2022).

76. What's more, it is no 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. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

77. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[27]

78. 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—Social Security number and name.

[27] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Oct. 17, 2022).

79. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[28]

80. 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.

81. 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.[29]

---

[28] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Oct. 17, 2022).

[29] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf (last visited Oct. 17, 2022).

82. Plaintiffs 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.

DEFENDANT FAILS TO COMPLY WITH FTC GUIDELINES

83. 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.

84. 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 customer 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 problems.[30]

[30] *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 (last visited Oct. 17, 2022).

85. 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.[31]

86. 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.

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

88. These FTC enforcement actions include actions against retail employers, like Defendant.

[31] *Id.*

89. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

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

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

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

DEFENDANT FAILS TO COMPLY WITH INDUSTRY STANDARDS

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

94. Several best practices have been identified that, at a minimum, should be implemented by retail 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.

95. Other best cybersecurity practices that are standard for retail 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.

96. 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.

97. These foregoing frameworks are existing and applicable industry standards for retail employers, 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

98. 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 Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) loss of time incurred due to actual identity theft; (e) loss of time due to increased spam and targeted marketing emails; (f) the loss of benefit of the bargain (price premium damages); (g) diminution of value of their PII; and (i) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as

Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

THE DATA BREACH INCREASES PLAINTIFFS AND CLASS MEMBER'S RISK OF IDENTITY THEFT

99. The unencrypted PII of Plaintiffs and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

100. Unencrypted PII may also fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Simply, unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

101. 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.

102. Plaintiffs' and Class Members' PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off their misfortune.

LOSS OF TIME TO MITIGATE THE RISK OF IDENTITY THEFT & FRAUD

103. 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.

104. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must, as Defendant's Notice Letter instructs them, "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.

105. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching the Data Breach's occurrence, reviewing their financial accounts for fraudulent activity, researching the credit and identity theft monitoring insurance offered by Defendant, and enrolling in credit and identity theft monitoring insurance.

106. 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."[32]

107. 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 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.[33]

108. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[34]

[32] *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.
[33] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 7, 2022).
[34] Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Sep 13, 2022).

109. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office 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."[35]

[35] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Sep. 13, 2022) ("GAO Report").

DIMINUTION OF VALUE OF PII

110. PII is a valuable property right.[36] 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.

111. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[37]

112. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[38] 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.[39,40] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[41]

---

[36] *See, e.g.,* John 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).

[37] *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/ (last visited Sep. 13, 2022).

[38] https://www.latimes.com/business/story/2019-11-05/column-data-brokers

[39] https://datacoup.com/

[40] https://digi.me/what-is-digime/

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

113. As a result of the Data Breach, Plaintiffs' 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 Plaintiffs 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.

114. Driver's license numbers are incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[42]

115. According to national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to

[42] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last accessed July 20, 2021)

> your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.[43]

116. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[44] However, this is not the case. As cybersecurity experts point out:

> "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks."[45]

117. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[46]

118. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs 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 Plaintiffs and Class Members as a result of a breach.

---

[43] Sue Poremba, *What Should I Do If My Driver's License Number is Stolen?"* (October 24, 2018) (last accessed July 20, 2021)

[44] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last accessed July 20, 2021)

[45] *Id.*

[46] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021 https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last accessed July 20, 2021)

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

120. Plaintiffs 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 .

121. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to potentially hundreds of thousands of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

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

FUTURE COST OF CREDIT AND IDENTITY THEFT MONITORING IS REASONABLE AND NECESSARY

123. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII, reports of misuse of Class Member PII 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.

124. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or his PII 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.

125. Consequently, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

126. 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. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their PII .

LOSS OF BENEFIT OF THE BARGAIN

127. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When submitting PII to Defendant under certain terms through a job application and/or onboarding paperwork, Plaintiffs 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, Plaintiffs and Class Members received an employment position of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

PLAINTIFF ANDREW SMITH'S EXPERIENCE

128. Prior to the Data Breach Plaintiff Smith was employed at Defendant for approximately twenty-four years, beginning in or about 1994. In the course of enrolling in employment with Defendant and as a condition of employment, he was required to supply Defendant with his PII, including but not limited to his name, address, date of birth, and Social Security number.

129. Plaintiff Smith is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

130. At the time of the Data Breaches—October 6, 2020, to December 8, 2021— Defendant retained Plaintiff Smith's PII in its system despite the fact that Plaintiff Smith was no longer employed by Defendant.

131. Plaintiff Smith received the Notice Letter, by U.S. mail, directly from Defendant, dated December 5, 2022. According to the Notice Letter, Plaintiff Smith's PII was improperly accessed and obtained by unauthorized third parties,

including his name, Social Security number, driver's license number, financial account information, and information related to his healthcare plan.

132. Upon receiving the Notice Letter form Defendant, Plaintiff Smith also spent time dealing with the consequences of the Data Breach, including time spent researching the Data Breach, reviewing his financial account for fraudulent activity, and enrolling in credit monitoring and identity theft insurance This time has been lost forever and cannot be recaptured.

133. Subsequent to the Data Breach, Plaintiff Smith has suffered numerous, substantial injuries including, but not limited to, (i) the diminution of the value of his PII (ii) loss of benefit of the bargain; and (iii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remain 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 his PII.

134. Plaintiff Smith additionally suffered actual injury and damages as a result of the Data Breach. Implied in his employment contract with Defendant was the requirement that it adequately safeguard his PII. Plaintiff Smith would not have worked for Defendant had Defendant disclosed that it lacked data security practices adequate to safeguard PII.

135. Plaintiff Smith further suffered actual injury in the form of damages and diminution in the value of his PII—a form of intangible property that he entrusted to Defendant for the purpose of employment, which was compromised by the Data Breach.

136. Plaintiff Smith also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number.

137. Plaintiff Smith has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen PII, especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

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

PLAINTIFF MACKENZIE FAIRFIELD'S EXPERIENCE

139. Prior to the Data Breach Plaintiff Fairfield was employed at Defendant for approximately eight months in or about 2018. In the course of enrolling in employment with Defendant and as a condition of employment, she was required to supply Defendant with her PII, including but not limited to her name, address, date of birth, and Social Security number.

140. Plaintiff Fairfield 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.

141. At the time of the Data Breaches—October 6, 2020, to December 8, 2021— Defendant retained Plaintiff Fairfield's PII in its system despite the fact that Plaintiff Fairfield was no longer employed by Defendant.

142. Plaintiff Fairfield received the Notice Letter, by U.S. mail, directly from Defendant, dated December 5, 2022. According to the Notice Letter, Plaintiff Fairfield's PII was improperly accessed and obtained by unauthorized third parties, including her name, Social Security number, driver's license number, financial account information, and information related to her healthcare plan.

143. Upon receiving the Notice Letter form Defendant, Plaintiff Fairfield also spent time dealing with the consequences of the Data Breach, including time spent researching the Data Breach, reviewing her financial accounts for fraudulent activity, and enrolling in credit monitoring and identity theft insurance. This time has been lost forever and cannot be recaptured.

144. Subsequent to the Data Breach, Plaintiff Fairfield has suffered numerous, substantial injuries including, but not limited to, (i) the diminution of

the value of her PII (ii) loss of benefit of the bargain; and (iii) 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) remain 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 her PII.

145. Plaintiff Fairfield additionally suffered actual injury and damages as a result of the Data Breach. Implied in her employment contract with Defendant was the requirement that it adequately safeguard her PII. Plaintiff Fairfield would not have worked for Defendant had Defendant disclosed that it lacked data security practices adequate to safeguard PII.

146. Plaintiff Fairfield further suffered actual injury in the form of damages and diminution in the value of her PII—a form of intangible property that she entrusted to Defendant for the purpose of employment, which was compromised by the Data Breach.

147. Plaintiff Fairfield also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy, especially her Social Security number.

148. Plaintiff Fairfield has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting

from her stolen PII, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

149. Plaintiff Fairfield 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

150. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

151. The Class that Plaintiffs seek to represent is defined as follows:

> All individuals residing in the United States whose PII was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Defendant on or about December 5, 2022 (the "Class").

152. 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 have 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.

153. Plaintiffs reserve the right to amend the definitions of the Class or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

154. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. At least 37,000 individuals were notified by Defendant of the Data Breach, according to the breach report submitted to Maine Attorney General's Office.[47] The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

155. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

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

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

[47] https://apps.web.maine.gov/online/aeviewer/ME/40/1af8a682-861a-4e94-a005-d50740ab143f.shtml

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

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

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

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

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs 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 Plaintiffs and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

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

156. 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.

157. 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 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.

158. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages he has suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

159. 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.

160. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs 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 Plaintiffs were 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.

161. 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.

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

163. 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.

164. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

165. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the Plaintiffs and the class of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

FIRST COUNT

Negligence
(On Behalf of Plaintiffs and the Class)

166. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 167 above as if fully set forth herein.

167. Defendant required Plaintiffs and Class Members to submit non-public PII as a condition of employment or as a condition of receiving employee benefits.

168. Plaintiffs and the Class Members entrusted their PII to Defendant with the understanding that Defendant would safeguard their information and delete it once it was no longer required to retain it after the end of the employment relationship.

169. Defendant had a duty to employ reasonable security measures and otherwise protect the PII of Plaintiffs and Class Members.

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

171. 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 safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

172. 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.

173. 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.

174. Defendant breached its duties, 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. Failing to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' PII; and

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

175. 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 in the industry.

176. 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.

177. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the PII and the harm suffered, or risk of imminent harm suffered by Plaintiffs and the Class.

178. As a result of Defendant's negligence, Plaintiffs and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, the costs associated therewith; time spent monitoring, addressing and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

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

180. Plaintiffs 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) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT

Intrusion Into Private Affairs / Invasion of Privacy (On Behalf of Plaintiffs and the Class)

181. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 167 above as if fully set forth herein.

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

183. Defendant owed a duty to Plaintiffs and Class Member to keep their PII confidential.

184. The unauthorized disclosure and/or acquisition (*i.e.,* theft) by a third party of Plaintiff's and Class Members' PII is highly offensive to a reasonable person.

185. Defendant's reckless and negligent failure to protect Plaintiff's and Class Members' PII constitutes an intentional interference with Plaintiffs' and the

Class Members' interest in solitude or seclusion, as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

186. Defendant's failure to protect Plaintiffs' and Class Members' PII acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

187. Defendant knowingly did not notify Plaintiffs and Class Members in a timely fashion about the Data Breach.

188. Because Defendant failed to properly safeguard Plaintiffs' and Class Members' PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

189. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiffs and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

190. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII is still maintained by Defendant with their inadequate cybersecurity system and policies.

191. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and

confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiffs and the Class.

192. Plaintiffs, on behalf of themselves and Class Members, seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class Members' PII.

193. Plaintiffs, on behalf of themselves and Class Members, seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

THIRD COUNT

Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

194. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 167 above as if fully set forth herein.

195. Plaintiffs and Class Members were required to provide their PII to Defendant as a condition of their employment with Defendant.

196. Plaintiffs and Class Members provided their labor to Defendant in exchange for (among other things) Defendant's promise to protect their PII from unauthorized disclosure and to delete it once it was no longer necessary to maintain the PII for employment purposes.

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

198. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' PII would remain protected.

199. Implicit in the agreement between Plaintiffs 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 Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

200. When Plaintiffs and Class Members provided their PII to Defendant as a condition of their employment or employee beneficiary status, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

201. Defendant required Class Members to provide their PII as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their PII to Defendant.

202. In entering into such implied contracts, Plaintiffs 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.

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

204. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

205. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PII.

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

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

208. Plaintiffs and Class Members are also entitled to nominal damages for the breach of implied contract.

209. Plaintiffs 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.

FOURTH COUNT

Negligence *Per Se*
(On Behalf of Plaintiffs and the Class)

210. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 167 above as if fully set forth herein.

211. Pursuant to Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' PII.

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

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

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

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

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

SIXTH COUNT

Breach of Confidence
(On Behalf of Plaintiffs and the Class)

217. Plaintiffs re-allege and incorporate by reference Paragraphs 1 through 167 above as if fully set forth herein.

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

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

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

221. Plaintiffs and Class Members also provided their PII to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure, such as following basic principles of protecting its networks and data systems, including employees' email accounts.

222. Defendant voluntarily received in confidence Plaintiffs and Class Members' PII with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

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

224. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and Class Members have suffered damages.

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

226. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs and Class Members' PII. Defendant knew its computer systems and technologies for accepting and securing Plaintiffs and Class Members' PII had numerous security vulnerabilities.

227. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: ((i) time spent researching the Data Breach; (ii) lost opportunity costs associated with effort expended and the loss of productivity addressing the Data Breach; (iii) time spent enrolling in credit and identity theft monitoring services; (iv) diminution in the value of their PII; (v) the continued risk to their PII, which remains 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; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (vii) the diminished value of Defendant's services they received.

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

SEVENTH COUNT

Violations of Georgia Uniform Deceptive Trade Practices Act, O.C.G.A. §§ 10-1-370 *et seq.*

229. Plaintiffs incorporate paragraphs 1 - 167 above as if fully set forth herein.

230. Plaintiffs and Class Members are "persons" within the meaning of O.C.G.A. § 10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA").

231. Defendant engaged in deceptive trade practices in the conduct of its business, in violation of Ga. Code § 10-1-372(a), including:

- Representing that goods or services have characteristics that they do not have;
- Representing that goods or services are of a particular standard, quality, or grade if they are of another;
- Advertising goods or services with intent not to sell them as advertised;
- Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

232. Defendants' deceptive trade practices include, *inter alia*:

a. Implementing and maintaining cybersecurity and privacy measures that were knowingly insufficient which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of individuals including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach and

d. Omitting, suppressing, and concealing the material fact that Defendant did not reasonably or adequately secure Plantiffs' PII.

233. Defendant's omissions were material because they were likely to and did deceive Plaintiffs and Class Members about the adequacy of Defendant's data security.

234. As a direct and proximate result of Defendant's actions, Plaintiffs and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages.

235. Plaintiffs and the Class Members seek all relief allowed by law, including injunctive relief and reasonable attorneys' fees and costs under Ga. Code § 10-1-373.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grants the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiffs and their 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 the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;

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

i. prohibiting 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 personal identifying information of Plaintiffs 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 Plaintiffs 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 Plaintiffs and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiffs 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 Plaintiffs and Class Members;

xii. requiring Defendant to conduct internal training and education routinely and continually, 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 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 PII 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 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;

D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees and costs

Pursuant to O.G.G.A. § 13-6-11 and as otherwise allowed by law;

F. For prejudgment interest on all amounts awarded; and

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

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all claims so triable.

Dated: January 25, 2023

Respectfully Submitted,

THE FINLEY FIRM, P.C.

By: /s/ *MaryBeth V. Gibson*
MaryBeth V. Gibson
Georgia Bar No. 725843
N. Nickolas Jackson
Georgia Bar No. 841433
3535 Piedmont Road
Building 14, Suite 230
Atlanta, GA 30305
Tel.: 404-320-9979
Fax: 404-320-9978
mgibson@thefinleyfirm.com
njackson@thefinleyfirm.com

Gary M. Klinger*
gklinger@milberg.com
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878

David K. Lietz*
dlietz@milberg.com
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
5101 Wisconsin Avenue NW, Suite 305
Washington D.C. 20016
Telephone: (202) 744-1795

Attorneys for Plaintiffs and the Proposed Class

*PRO HAC VICE FORTHCOMING

CERTIFICATE OF COMPLIANCE

I certify that the foregoing pleading has been prepared with Times New Roman, 14-point font, in compliance with L.R. 5.1B.

/s/ MaryBeth V. Gibson
MARYBETH V. GIBSON

ClassAction.org
