UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF NORTH CAROLINA

Veronica Roman, *on behalf of herself and all others similarly situated,* Plaintiff, v. Hanesbrands, Inc., Defendant.	**Case No.** **COMPLAINT — CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiff Veronica Roman ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendant Hanesbrands, Inc. ("Hanes" or "Defendant") as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels' investigation, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. This class action arises out of the recent cyberattack and data breach ("Data Breach") that was perpetuated against Hanes, an international clothing and apparel business, which collected and maintained certain personally identifiable information ("PII") of Plaintiff and the putative Class Members (defined below), who are (or were) employees at Hanes.

2. As a result of the Data Breach, Plaintiff and potentially thousands of Class Members, suffered concrete injury in fact including, but not limited to: eviction, due to fraudulent activity under her name; denial of an automobile-financing loan; over $15,000

of fraudulent charges; and identity theft that resulted in the unauthorized party attempting to open new financial accounts under her name.

3. Plaintiff and Class Members also suffered ascertainable losses in the form of the loss of the benefit of their bargain, lost value of their PII, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

4. Plaintiff's and Class Members' sensitive personal information—which was entrusted to Defendant—was compromised and unlawfully accessed due to the Data Breach.

5. The private information compromised in the Data Breach included first and last names, Social Security numbers (the holy grail for identity thieves), dates of birth, government-issued identification numbers (such as driver's license numbers), addresses, information related to benefits and employment including certain health information, and financial account information (collectively, "Private Information").

6. The Private Information compromised in the Data Breach was exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals.

7. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its employees' Private Information.

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

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

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

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

11. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct because the Private Information that Defendant collected and maintained is now in the hands of data thieves.

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

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

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

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

16. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including

improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

17. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct.

II. PARTIES

18. Plaintiff Veronica Roman is and has been at all relevant times a resident and citizen of California, currently residing in Beaumont, California. She is a former employee at Defendant and worked there for approximately eight months in or about 2011. As a condition of Plaintiff's employment at Hanes, she was required to provide her PII to Defendant. Plaintiff received the Notice of Data Breach letter, directly from Defendant, via U.S. mail, dated September 30, 2022 (the "Notice Letter"). If Ms. Roman 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.

19. Defendant Hanesbrands, Inc. is an international clothing and apparel company incorporated under the state laws of Maryland and headquartered in North Carolina with its principal office located at 1000 E. Hanes Mill Road, Winston Salem, North Carolina, 27105. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known. All of Plaintiff's claims stated herein are

asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because many putative class members, including Plaintiff, are citizens of a different state than Defendant. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

21. This Court has personal jurisdiction over Defendant because it operates and maintains its principal place of business in this District and the computer systems implicated in this Data Breach are likely based in this District. Further, Defendant is authorized to and regularly conducts business in this District and makes decisions regarding corporate governance and management of its businesses in this District, including decisions regarding the security measures to protect its customers' PII. By promoting, selling and marketing its products and services from North Carolina to thousands of consumers nationwide, Defendant intentionally avails itself of this jurisdiction.

22. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because a substantial part of the events giving rise to this action occurred in this District,

including decisions made by Defendant's governance and management personnel or inaction by those individuals that led to the Data Breach; Defendant's principal place of business is located in this district; Defendant maintains Class Members' PII in this District; and Defendant caused harm to Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

Background

23. Defendant is an international clothing and apparel company that sells its products "everywhere consumers shop: at mass-merchandise, mid-tier, department-store, college bookstores, dollar-stores, food and drug, and club-store retailers, as well as directly to consumers via the Internet and nearly 1,000 company-owned retail stores worldwide."[1] Defendant currently "employs 59,000 associates in 33 countries".[2]

24. Upon information and belief, in the course of collecting Private Information from employees, including Plaintiff, 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.

25. Defendant made these promises in, among other things, its Global Code of Conduct available to the public online.[3] In the "Private Information" section of Global Code of Conduct,[4] Defendant states it "respect[s] the privacy of employees", and that "Data

[1] https://newsroom.hanesbrands.com/corporate-fact-sheet/default.aspx
[2] *Id.*
[3] https://ir.hanesbrands.com/static-files/6e86ca4a-3afb-42a8-80e1-abb0da78142e
[4] In its Global Code of Conduct, Defendant defines 'personal information' as "[a]ny information relating to an identified or identifiable natural person." *Id.*

privacy laws cover how we must collect, store, use, share, transfer and dispose of personal information, and *we comply with those laws everywhere we operate*."[5]

26. Plaintiff and the Class Members, as former and current Defendant employees relied on these promises and on this sophisticated business entity to keep their sensitive PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Employees, in general, demand security to safeguard their PII, especially when Social Security numbers and other sensitive PII is involved.

27. In the course of their employment relationship, employees, including Plaintiff and Class Members, provided Defendant with at least the following Private Information:

a. names;

b. dates of birth;

c. Social Security numbers;

d. addresses;

e. government-issued identification numbers; and,

f. financial account information.

28. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

[5] *Id.* (Emphasis added).

29. In the Notice Letter sent to Plaintiff and Class Members, Defendant asserts that on May 24, 2022, it "detected a ransomware incident impacting certain internal IT systems" and determined that "some of [Plaintiff's and Class Member's] information was impacted in the event."

30. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, whether Defendant's system is still unsecured, why it took over four months to inform impacted individuals after Defendant first detected the Data Breach, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

31. Upon information and belief, Plaintiff's and Class Members' information was, in fact, involved in a data security incident.

32. Upon information and belief, the cyberattack was targeted at Defendant, due to its status as an employer that collects, creates, and maintains PII on its computer networks and/or systems.

33. Because of this targeted cyberattack, data thieves were able to gain access to and obtain data from Defendant that included the Private Information of Plaintiff and Class Members.

34. The files, containing Plaintiff's and Class Members' Private Information and stolen from Defendant, included the following: "contact information, date of birth,

financial account information, government issued identification numbers such as drivers' license numbers, passport information and social security numbers; and other information related to benefits and employment, including certain limited health information provided for employment-related purposes."

35. Defendant confirmed that the Data Breach was the result of a ransomware attack but has failed to indicate whether the compromised information was retrieved or if it remains in the hands of cybercriminals.

36. Ransomware attacks, like that experienced by Defendant, are a well-known threat to companies that maintain Private Information. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue".[6] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."

37. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data contained within.[7] In 2020, over 50% of ransomware attackers exfiltrated data

[6] *Ransomware: The Data Exfiltration and Double Extortion Trends*, available at https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends

[7] *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/

from a network before encrypting it.[8] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt."[9] And even where companies pay for the return of data attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[10]

38. As evidenced by the fraud and identity theft experienced by Plaintiff following the Data Breach, the Private Information contained in Defendant's network was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated unintelligible data.

39. Plaintiff's Private Information was accessed and stolen in the Data Breach and Plaintiff believes her stolen Private Information is currently available for sale on the dark web because that is the *modus operandi* of cybercriminals.

40. Defendant admits in the Notice Letter that Plaintiff's Private Information "was impacted in the event."[11]

41. Due to the actual and imminent risk of identity theft as a result of the Data Breach, Plaintiff and Class Members must, as the Notice Letter instructs them, "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.[12] Defendant further encouraged Plaintiff and Class Members to monitor

[8] 2020 Ransomware Marketplace Report, available at https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*

their financial accounts by providing 24 months of credit and identity monitoring services to do so.[13]

42. That Defendant is encouraging its current and former employees to enroll in credit monitoring and identity theft restoration services is an acknowledgment that the impacted individuals are subject to a substantial and imminent threat of fraud and identity theft.

43. Defendant had obligations created by contract, state and federal law, common law, and industry standards to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

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

45. Defendant also failed to give timely and adequate notice of the Data Breach. Defendant admits that the breach was discovered on May 24, 2022, but Defendant did not send a Notice Letter to Plaintiff and Class Members until September 30, 2022—*more than four months* after Defendant detected the Data Breach.

46. The unencrypted Private Information of Plaintiff and Class Members may end up for sale to identity thieves on the dark web, if it has not already, or it could simply fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members.

[13] *Id.*

Unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

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

48. 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."[14]

49. 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.

[14] 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 Oct. 17, 2022).

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[15]

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

50. 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….

- **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….[16]

51. 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;

[16] *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).

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].[17]

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

53. 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 thousands of current and former employees, including Plaintiff and Class Members.

Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' Private Information.

54. Defendant acquires, collects, and stores a massive amount of Private Information on its employees, former employees and other personnel.

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

[17] *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).

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

57. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

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

Defendant Knew or Should Have Known of the Risk of the Risk Because Employers in Possession of PII are Particularly Suspectable to Cyber Attacks

59. 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 Private Information, like Defendant, preceding the date of the breach.

60. Data breaches, including those perpetrated against employers that store PII in their systems, have become widespread. In 2019, a record 1,473 data breaches occurred, resulting in approximately 164,683,455 sensitive records being exposed, a 17% increase from 2018.[18]

[18] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Year-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last accessed Oct. 17, 2022).

61. The 525 reported breaches reported in 2019 exposed nearly 40 million sensitive records (39,378,157), compared to only 369 breaches that exposed just over 10 million sensitive records (10,632,600) in 2018.[19]

62. 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 Private Information are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[20]

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

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

---

[19] *Id.* at p15.

[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).

65. Defendant's knowledge of the foreseeable risk of a cyber-attack, like the one experienced by Defendant, is demonstrated by Defendant's Global Code of Conduct, which provides that: "[w]e are all increasingly dependent on networks, databases and the information they contain and transmit. Hacks, intentional breaches and lax security are risks that we are all aware of and that we are right to worry about. *Companies gather enormous amounts of personal data and consequently have an increased responsibility to protect that information*. Each of us must do our part[.]"[21] (Emphasis added).

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

67. In the Notice Letter, Defendant makes an offer of 24 months of identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' Private Information.

[21] https://ir.hanesbrands.com/static-files/6e86ca4a-3afb-42a8-80e1-abb0da78142e#:~:text=We%20always%20obey%20the%20law,of%20HanesBrands%20and%20our%20success.

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

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

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

Value of Personally Identifiable Information

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

[22] 17 C.F.R. § 248.201 (2013).

registration number, government passport number, employer or taxpayer identification number."[23]

72. 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 pricing for stolen identity credentials.[24] For example, Personal Information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[25] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web. Criminals can also purchase access to entire company data breaches from $900 to $4,500.[26]

73. Social Security numbers, which were compromised for some of the Class Members as alleged herein, for example, 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 is the case here, 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

[23] *Id.*
[24] *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).
[25] *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).
[26] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Oct. 217, 2022).

> 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.[27]

74. 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.

75. 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."[28]

76. 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, name, and date of birth.

---

[27] 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).
[28] 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).

77. 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."[29]

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

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[30]

Defendant Fails to Comply with FTC Guidelines

80. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data

[29] Time 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).
[30] *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).

security practices. According to the FTC, the need for data security should be factored into all business decision-making.

81. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal employee information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[31]

82. 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.[32]

83. The FTC further recommends that companies not maintain Private Information 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.

[31] *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).
[32] *Id.*

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

85. These FTC enforcement actions include actions against employers over the compromised Private Information of its employees, like Defendant here. *See, e.g., Purvis v. Aveanna Healthcare, LLC,* 563 F.Supp.3d 1360, 1374 (N.D. Ga. 2021) (Court finding plaintiff adequately alleged negligence claim based upon violation of Section 5 of the FTC Act).

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

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

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

Defendant Fails to Comply with Industry Standards

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

90. Several best practices have been identified that a minimum should be implemented by employers in possession of Private Information, 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.

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

92. 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.

93. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to its employees with respect to data privacy. 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

94. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (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) "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) the loss of benefit of the bargain (price premium damages); (j) diminution of value of their Private Information; and (k) 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' Private Information.

The Data Breach Increases Plaintiff's and Class Member's Risk of Identity Theft

95. In addition to the identity theft already suffered by Plaintiff, Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

96. The unencrypted Private Information of Plaintiff and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiff and Class Members.

97. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information 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.

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

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

Loss of Time to Mitigate the Risk of Identity Theft and Fraud

100. 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 Private Information 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.

101. Thus, due to the actual and imminent risk of identity theft, Plaintiff 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.

102. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with

credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

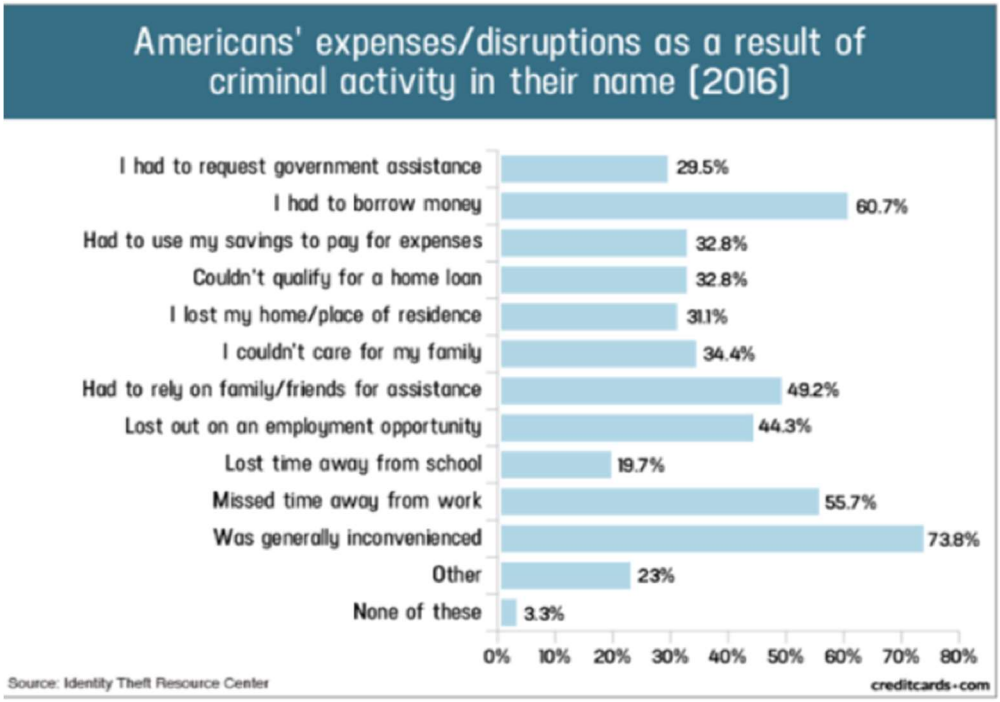
103. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[33]

104. 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.[34]

105. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[35]

---

[33] *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.
[34] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 7, 2022).
[35] 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).



106. 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."[36]

Diminution Value of Private Information

107. Private Information is a valuable property right.[37] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber

[36] *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").

[37] *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).

thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

108. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals and other entities in custody of PII often purchase PII on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PII to adjust their insureds' medical insurance premiums.

109. An active and robust legitimate marketplace for Private Information 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]

110. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[42]

111. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets,

[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
[42] *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).

has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

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

113. 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.

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

115. Driver's license numbers, which was compromised for some Class Members' in the Data Breach, are also 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."[43]

116. 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 your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.[44]

117. 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."[45] 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.[46]

118. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[47]

---

[43] 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)
[44] Sue Poremba, *What Should I Do If My Driver's License Number is Stolen?"* (October 24, 2018) (last accessed July 20, 2021)
[45] 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)
[46] *Id.*
[47] *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. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

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

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

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

123. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information, reports of misuse of Class Member Private Information 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 Private Information 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 her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

125. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[48] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

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

127. 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

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

Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

Loss of the Benefit of the Bargain

128. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When submitting Private Information to Defendant under certain terms through a job application and/or onboarding paperwork, Plaintiff and other reasonable employees understood and expected that Defendant would properly safeguard and protect their Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff 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 Roman's Experience

129. Prior to the Data Breach Plaintiff Roman was employed at Defendant for approximately eight months in or about 2011. In the course of enrolling in employment with Defendant and as a condition of employment, she was required to supply Defendant with her Private Information, including but not limited to her name, address, date of birth, and Social Security number.

130. Plaintiff Roman is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe

and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

131. On the day of the Data Breach—May 24, 2022— Defendant retained Plaintiff's Private Information in its system, despite not having any relationship with Plaintiff in the ten years preceding the Data Breach.

132. Plaintiff Roman received the Notice Letter, by U.S. mail, directly from Defendant, dated September 30, 2022. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including potentially all of the following: "contact information; date of birth; financial account information; government issued identification numbers such as drivers' license numbers, passport information and social security numbers; and other information related to benefits and employment, including certain limited health information provided for employment-related purposes."

133. Upon receiving the Notice Letter form Defendant, Plaintiff Roman also spent time dealing with the consequences of the Data Breach, including time spent verifying the legitimacy of the Notice Letter, enrolling in credit monitoring and identity theft insurance options, contacting her bank regarding fraudulent charges and financial accounts being opened under her name, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

134. Subsequent to the Data Breach, Plaintiff Roman has suffered numerous, substantial injuries including, but not limited to: (1) eviction from her residence, due to

fraudulent activity occurring under her name; (2) denial for a loan to purchase a vehicle, due to fraudulent activity under her name; (3) over $15,000 of fraudulent purchases; (4) fraudulent attempts to open new financial accounts under her name; and (5) identity theft.

135. Plaintiff Roman 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 Private Information. Plaintiff Roman would not have worked for Defendant had Defendant disclosed that it lacked data security practices adequate to safeguard Private Information.

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

137. Plaintiff Roman 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.

138. Plaintiff Roman has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her stolen Private Information, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

139. Plaintiff Roman has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

140. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated.

141. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons whose Private Information was maintained on Defendant's computer systems that were compromised in the Data Breach and who were sent Notice of the Data Breach letter from Defendant (the "Class").

142. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

143. Plaintiff hereby reserves the right to amend or modify the Class definitions with greater specificity or division after having had an opportunity to conduct discovery.

144. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff

at this time, based on information and belief, the Class consists at least multiple thousand persons whose data was compromised in Data Breach.[49]

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

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. 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;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

[49] According to the Maine Attorney General, approximately 109 Maine residents were impacted. Given Defendant's large presence in conjunction with the relatively small population in Maine, it can be inferred that the Data Breach impacted at least multiple thousand persons. *See* https://apps.web.maine.gov/online/aeviewer/ME/40/6f9be6c4-7e0f-4015-a7b1-1d6dcc66ccd1.shtml

g. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant breached implied contracts for adequate data security with Plaintiff and Class Members;

l. Whether Defendant was unjustly enriched by retention of the monetary benefits conferred on it by Plaintiff and Class Members;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

146. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

147. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

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

149. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

150. 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.

151. Likewise, particular issues under Fed. R. Civ. P. 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 owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

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

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

d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

e. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

152. Finally, all Members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice of the Data Breach by Defendant.

VI. CLAIMS

COUNT I
Negligence
(On behalf of Plaintiff and the Class)

153. Plaintiff realleges and incorporates by reference all allegations above and below as though fully stated herein.

154. Defendant required Plaintiff and Class Members to submit non-public Private Information as a condition of employment or as a condition of receiving employee benefits.

155. Plaintiff and the Class Members entrusted their PII to Defendant with the understanding that Defendant would safeguard their information and delete it once the employment relationship terminated.

156. Defendant's knowledge of the foreseeable risk of a cyber-attack, like the one experienced by Defendant, is demonstrated by Defendant's Global Code of Conduct, which states: "[w]e are all increasingly dependent on networks, databases and the information they contain and transmit. Hacks, intentional breaches and lax security are risks that we are all aware of and that we are right to worry about. *Companies gather enormous amounts of personal data and consequently have an increased responsibility to protect that information*. Each of us must do our part[.]"[50]

[50] *See* https://ir.hanesbrands.com/static-files/6e86ca4a-3afb-42a8-80e1-abb0da78142e#:~:text=We%20always%20obey%20the%20law,of%20HanesBrands%20and%20our%20success. (Emphasis added).

157. 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.

158. 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.

159. 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 Private Information.

160. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. 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' Private Information;

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' Private Information; and

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

161. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information 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.

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

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

164. As a result of Defendant's negligence, Plaintiff and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: eviction due to fraudulent activity; denial for an automobile loan due to fraudulent activity; attempted fraudulent charges and financial accounts being opened; identity theft; 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.

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

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

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

167. Plaintiff re-alleges and incorporates by reference all allegations above and below as if fully set forth herein.

168. Plaintiff and Class Members were required to provide their Private Information to Defendant as a condition of their employment with Defendant.

169. Plaintiff and Class Members provided their labor to Defendant in exchange for (among other things) Defendant's promise to protect their Private Information from unauthorized disclosure.

170. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff

and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

171. Defendant's Global Code of Conduct states: "Data privacy laws cover how we must collect, store, use, share, transfer and dispose of personal information, and we comply with those laws everywhere we operate."[51]

172. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' Private Information would remain protected.

173. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide Private Information, was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential, and (g) delete or destroy Private Information after it was no longer necessary to retain for employment obligations.

[51] https://ir.hanesbrands.com/static-files/6e86ca4a-3afb-42a8-80e1-abb0da78142e#:~:text=We%20always%20obey%20the%20law,of%20HanesBrands%20and%20our%20success.

174. When Plaintiff and Class Members provided their Private Information 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 and to delete or destroy it following the end of the employment relationship.

175. Defendant required Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

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

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

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

179. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

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

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

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

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

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

184. Plaintiff re-alleges and incorporates by reference all allegations above and below as if fully set forth herein.

185. Plaintiff alleges Count III solely in the alternative to Count II.

186. Plaintiff and Class Members conferred a monetary benefit on Defendant by providing Defendant with labor for Defendant's business.

187. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiff and Class Members and accepted that monetary benefit.

188. However, acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Defendant to retain that benefit without payment of

the value thereof. Specifically, Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

189. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures.

190. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

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

192. Plaintiff and Class Members have no adequate remedy at law. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered or will suffer injury, including but not limited to: eviction due to fraudulent activity; denial for an automobile loan due to fraudulent activity; attempted fraudulent charges and financial accounts being opened; identity theft; 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; the necessity to engage legal counsel and incur attorneys' fees, costs and expenses; and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

193. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

194. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

COUNT IV
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

195. Plaintiff realleges and incorporates by reference all allegations above and below as though fully stated herein.

196. Defendant's conduct constitutes negligence *per se* because it was in violation Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored, and the foreseeable consequences

of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiff and Members of the Class due to the valuable nature of the Private Information at issue in this case—including Social Security numbers.

197. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

198. Plaintiff and members of the Class are within the class of persons that the FTC Act was intended to protect.

199. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against employers, which, as a result of failures to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm to its employees as that suffered by Plaintiff and members of the Class.

200. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences

of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the Private Information of its current and former employees and customers in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and members of the Class.

201. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and members of the Class have suffered and will suffer the continued risks of exposure of their Private Information, 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 Private Information in their continued possession.

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

203. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages

204. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's Private Information.

205. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant,[52] of failing to use reasonable measures to protect Private Information. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff and the members of the Class's sensitive Private Information.

206. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result in the event of a breach, which ultimately came to pass.

[52] https://www.ftc.gov/news-events/news/press-releases/2011/05/ftc-settles-charges-against-two-companies-allegedly-failed-protect-sensitive-employee-data

207. Defendant had a duty to Plaintiff and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Class's Private Information.

208. Defendant breached its respective duties to Plaintiff and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and members of the Class's Private Information.

209. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence *per se.*

210. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

211. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of their duties. As evidenced in its Global Code of Conduct,[53] Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their Private Information.

[53] The Global Code of Conduct provides: "Hacks, intentional breaches and lax security are risks that we are all aware of and that we are right to worry about. Companies gather enormous amounts of personal data and consequently have an increased responsibility to protect that information. Each of us must do our part[.]" *See https://ir.hanesbrands.com/static-files/6e86ca4a-3afb-42a8-80e1-abb0da78142e#:~:text=We%20always%20obey%20the%20law,of%20HanesBrands%20and%20our%20success.*

212. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of Private Information; fraudulent charges to credit and/or debit cards; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT VI
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

213. Plaintiff re-alleges and incorporates by reference all allegations above and below as if fully set forth herein.

214. Plaintiff and Class Members had a legitimate expectation of privacy regarding their Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

215. Defendant owed a duty to Plaintiff and Class Member to keep their Private Information confidential.

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

217. Defendant's reckless and negligent failure to protect Plaintiff's and Class Members' Private Information constitutes an intentional interference with Plaintiff's and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

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

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

220. Because Defendant failed to properly safeguard Plaintiff's and Class Members' Private Information, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

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

222. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their Private Information are still maintained by Defendant with their inadequate cybersecurity system and policies.

223. Plaintiff 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 Private Information of Plaintiff and the Class.

224. Plaintiff, on behalf of herself and Class Members, seeks injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' Private Information.

225. Plaintiff, on behalf of herself and Class Members, seeks 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.

COUNT V
Violation of North Carolina's Unfair and Deceptive Trade Practices Act
(On Behalf of Plaintiff and the Class)

226. Plaintiff realleges and incorporates by reference all the allegations above and below above as though fully stated herein.

227. The North Carolina Unfair and Deceptive Trade Practices Act ("NCUDTPA") prohibits "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce[.]" N.C. Gen. Stat. § 75-1.1(a).

228. Under the act, "commerce" includes "all business activities, however, denominated[.]" *Id.* at § 75-1.1(b).

229. Defendant is a corporation that owns, maintains, and records Private Information, and computerized data including Private Information, about its current and former employees, including Plaintiff and Class members.

230. Furthermore, "any person . . . injured . . . by reason of any act or thing done by any other person, firm or corporation in violation of this Chapter, such person . . . so injured shall have a right of action on account of such injury done[.]" *Id.* at § 75-16.

231. Defendant's conduct was unfair and deceptive in violation of the NCUDTPA. Specifically, Defendant represented that it could adequately protect employees' Private Information and that its platforms were safe and secure. It solicited employees' labor through these representations and, in turn, gained Plaintiff and the Class decided to accept employment from Defendant.

232. Defendant, however, could not adequately protect its employees' Private Information, and designed an insecure platform lacking reasonable data security measures that were entirely inadequate to protect the highly sensitive data it collected and stored.

233. Defendant is in possession of PII belonging to Plaintiff and Class members and is responsible for notifying "affected person[s] that there has been a security breach following discovery. . . of the breach." N.C. Gen. Stat. Ann. § 75-65(a).

234. Under N.C. Gen. Stat. §§ 75-61, 75-65, businesses impacted by a data breach must provide notice without reasonable delay. Defendant, however, waited over four months to notify Plaintiff and Class of Data Breach's occurrence.

235. Upon detecting the Data Breach on May 24, 2022, Defendant failed to provide timely and adequate notice of the Data Breach's occurrence to Plaintiff and Class Members.

236. Defendant's conduct was, thus, unethical, unscrupulous, substantially injurious to its employees, and against North Carolina's stated policy of quickly providing notice of a data breach.

237. Defendant's conduct was also in and affecting commerce because it concerned the labor supply available to other companies. Specifically, by misrepresenting its data security so as to acquire Plaintiff's and the Class' consent for employment, Defendant's misconduct resulted in a diminished supply of employees available, as Plaintiff and Class Members would have become employed by another company instead of Defendant.

238. Any benefit resulting from Defendant's acts and omissions is outweighed by the harm to Plaintiff and Class Members.

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

240. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members suffered and continue to suffer injuries and are entitled to damages in an amount to be proven at trial.

241. Plaintiff seeks actual and compensatory damages, injunctive relief, attorneys' fees and expenses, and all other remedies available under the law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grant the following:

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

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

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

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

ii. requiring Defendant to protect, including through encryption, all data collected through the course of their 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 Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

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

v. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

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

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

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

ix. requiring Defendant to conduct regular database scanning and securing checks;

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

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal

security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

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

xiii. 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;

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

xv. 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 actual damages, compensatory damages, statutory damages, and nominal damages, in an amount to be determined, as allowable by law;

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

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

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

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

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Dated: January 16, 2023

Respectfully submitted,

/s /Scott C. Harris

Scott C. Harris (SBN 35328)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
900 W. Morgan Street
Raleigh, North Carolina 27603
Phone: (919) 600-5000
sharris@milberg.com

Counsel for Plaintiff and the Proposed Class