UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF GEORGIA
SAVANNAH DIVISION

SABRINA GREEN-FOGG, on behalf of herself and all others similarly situated, Plaintiff, v. CITI TRENDS, INC., Defendant.	)	Case No. CV423-196 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

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

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personal identifiable information ("PII") of Defendant's current and former employees and prospective employees, including, but not limited to, first and last name, Social Security number, date of birth, bank /financial account number, routing number, and other information.

2. Defendant is a clothing retailer that has been in business for "over 75 years" and currently operates "over 600+ stores in 33 states."[1]

3. Upon information and belief, prior to and through January 14, 2023, Defendant obtained the PII of Plaintiff and Class Members, including by collecting it directly from Plaintiff and Class Members.

4. Upon information and belief, prior to and through January 14, 2023, Defendant stored the PII of Plaintiff and Class Members, unencrypted, in an Internet-accessible environment on Defendant's network.

5. On or around January 14, 2023, Defendant learned of a data breach on its network that occurred on or around January 14, 2023 (the "Data Breach").

6. Defendant determined that, during the Data Breach, an unknown actor accessed files containing the PII of Plaintiff and Class Members.

7. On or around February 23, 2023, Defendant filed a Form 8-K with the Security and Exchange Commission stating that the Data Breach was the result of a "Hive ransomware" attack.

8. On or around June 21, 2023, Defendant began notifying various states Attorneys General of the Data Breach.

9. On or around June 21, 2023, Defendant began notifying Plaintiff and Class Members of the Data Breach.

[1] https://cititrends.com/about-us/ (last visited July 13, 2023).

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

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

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

13. Plaintiff and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (a) Plaintiff experiencing fraud in the form on a Bank of America account being falsely opened in her name in or about January 2023; (b) Plaintiff's out-of-pocket costs spent on LifeLock credit monitoring and identity theft protection services; (c) Plaintiff experiencing an increase in spam calls, texts, and/or emails since the Data Breach; (d) invasion of privacy; (e) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (f) the loss of benefit of the bargain (price premium damages); (g) diminution of value of their PII; and (h) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

14. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party.

15. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to damages and injunctive and other equitable relief.

PARTIES

16. Plaintiff Sabrina Green-Fogg is and has been, at all relevant times, a resident and citizen of Allentown, Pennsylvania. Ms. Green-Fogg received the Notice Letter, via U.S. mail, directly from Defendant, dated June 22, 2023. Ms. Green-Fogg provided her PII to Defendant on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect her PII. If Ms. Green-Fogg 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.

17. Defendant Citi Trends, Inc. is a Delaware corporation with its principal place of business located at 104 Coleman Boulevard, Savannah, Georgia 31408.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiff Green-Fogg, is a citizen of a state different from Defendant.

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

20. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

FACTUAL ALLEGATIONS

Defendant's Business

21. Defendant is a clothing retailer that has been in business for "over 75 years" and currently operates "over 600+ stores in 33 states."[2]

22. Plaintiff and Class Members are current and former employees at Defendant.

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

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

[2] https://cititrends.com/about-us/ (last visited July 13, 2023).

25. Upon information and belief, in the course of collecting PII 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.

26. Indeed, Defendant's Privacy Policy provides that: "[w]e have implemented reasonable measures designed to secure your personal information from accidental loss and from unauthorized access, use, alteration, and disclosure."[3]

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

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

[3] https://cititrends.com/privacy-policy/ (last visited July 13, 2023).

29. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep employees' PII safe and confidential.

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

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

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

The Data Breach

33. On or about June 22, 2023, Defendant sent Plaintiff and other victims of the Data Breach a Notice of Security Incident letter (the "Notice Letter"), informing them that:

> **What happened?** On or about January 14, 2023, a third-party entered and disrupted our information technology network. We immediately investigated and responded swiftly to this event, changing passwords and blocking the unauthorized access. Outside technical experts were also engaged to enhance the security of our systems.

> **What information was involved?** This unauthorized third-party had the ability to extract data from our IT environment, including certain files containing employee and prospective employee information. Based upon the results of the investigation, Citi Trends undertook an extensive process of reviewing the potentially impacted files for sensitive information. While we do not have any evidence that anyone has actually obtained and misused your information, we are notifying you out of an abundance of caution that the potentially impacted files may have included your first and last name, Social Security Number, Date of Birth, Bank / Financial Account Information, Routing Number, and other information you may have shared with us in connection with your employment. We recommend that you remain vigilant and follow the steps below.[4]

34. Omitted from the Notice Letter were the date that Defendant discovered the Data Breach, any explanation as to why it took Defendant more than *five months* after the cyberattack's occurrence to inform Plaintiff and Class Members of the Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these critical facts have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

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

[4] https://apps.web.maine.gov/online/aeviewer/ME/40/07c5c0b1-c0bc-4579-bfb6-697b4bfd4e4b.shtml (last visited July 13, 2023).

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

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

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

Data Breaches Are Preventable

39. 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."[5]

40. 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:

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

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

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

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

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

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

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

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

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

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

41. To prevent and detect cyber-attacks or ransomware attacks Citi Trends 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

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

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

Apply principle of least-privilege

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

Harden infrastructure

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

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

43. 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 that of Plaintiff and Class Members.

Defendant Acquires, Collects, And Stores Employees' PII

[7] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Nov. 11, 2021).

44. As a condition of becoming an employee at Defendant, Plaintiff and Class Members were required to give their sensitive and confidential PII to Defendant.

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

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

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

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

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

50. Indeed, Defendant's Privacy Policy provides that: "[w]e have implemented reasonable measures designed to secure your personal information from accidental loss and from unauthorized access, use, alteration, and disclosure."[8]

Defendant Knew, Or Should Have Known, of the Risk Because Employers In Possession Of PII Are Susceptible To Cyber Attacks

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

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

53. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew

[8] https://cititrends.com/privacy-policy/ (last visited July 13, 2023).

or should have known that the PII that they collected and maintained would be targeted by cybercriminals.

54. Additionally, as companies became more dependent on computer systems to run their business,[9] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[10]

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

56. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[11]

[9]https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html
[10] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022
[11] *See* 2021 Data Breach Annual Report (ITRC, Jan. 2022) (available at https://notified.idtheftcenter.org/s/), at 6.

57. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[12]

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

59. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[13]

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

---

[12] *Id*.

[13] 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).

61. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially thousands of individuals' detailed, PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

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

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

64. 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.

65. 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.

66. As an employer in possession of its current and former employees' PII, Defendant knew, or should have known, the importance of safeguarding the PII entrusted to them by 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. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

Value of Personally Identifying Information

67. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[14] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[15]

[14] 17 C.F.R. § 248.201 (2013).
[15] *Id.*

68. 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.[16] For example, Personal Information can be sold at a price ranging from $40 to $200.[17] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[18]

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

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[19]

---

[16] *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).

[17] *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).

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

[19] 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).

70. 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.

71. 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."[20]

72. 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— i.e., Social Security numbers and names. Because the information compromised in the Data

[20] 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).

Breach is immutable, Plaintiff and Class Members are at risk of identity theft and fraud for the remainder of their lives.

73. 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."[21]

74. 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.

75. 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,

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

> studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[22]

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

Defendant Fails To Comply With FTC Guidelines

77. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

78. 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

[22] *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).

their network's vulnerabilities; and implement policies to correct any security problems.[23]

79. 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.[24]

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

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

[23] *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).
[24] *Id.*

these actions further clarify the measures businesses must take to meet their data security obligations.

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

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

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

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

86. Upon information and belief, Citi Trends was at all times fully aware of its obligation to protect the PII of its employees, Citi Trends was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

Defendant Fails To Comply With Industry Standards

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

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

89. 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. Citi Trends failed to follow these cybersecurity best practices, including failure to train staff.

90. 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.

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

Common Injuries & Damages

92. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; and € the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further

breaches, so long as Citi Trends fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

Data Breaches Increase Victims' Risk Of Identity Theft

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

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

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

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

97. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[25]

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

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

[25] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on May 26, 2023).

a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

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

101. Thus, even if certain information (such as emails or telephone numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

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

Loss Of Time To Mitigate Risk Of Identity Theft & Fraud

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

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

105. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as changing passwords and resecuring their own computer systems, filing police reports relating to fraudulent activity, contacting financial institutions to sort out fraudulent activity, pulling credit reports, filing complaints with the FTC, contacting the IRS to secure their accounts, signing up for credit monitoring and identity theft protection, and contacting credit bureaus to place credit alerts on their accounts.

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

107. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven

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

years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[27]

108. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[28]

109. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity

[27] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 7, 2022).
[28] 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).

theft will face "substantial costs and time to repair the damage to their good name and credit record."[4]

Diminution of Value of PII

110. PII is a valuable property right.[29] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

111. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[30]

112. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[31] 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

[29] *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").
[30] *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).
[31] *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).

provides it to marketers or app developers.[32,33] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[34]

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

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

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

116. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is

[32] https://www.latimes.com/business/story/2019-11-05/column-data-brokers
[33] https://datacoup.com/
[34] https://digi.me/what-is-digime/

incurring and will continue to incur such damages in addition to any fraudulent use of their PII .

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

118. 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

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

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

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

122. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their PII.

Loss Of Benefit Of The Bargain

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

employment position of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff Sabrina Green-Fogg's Experience

124. Plaintiff Sabrina Green-Fogg was employed by Defendant from approximately 2012 to 2014.

125. In the course of enrolling in employment with Defendant and as a condition of employment, she was required to supply Defendant with her PII, including but not limited to: her name, financial information, date of birth, and Social Security number.

126. At the time of the Data Breach—on or about January 14, 2023—Citi Trends retained Plaintiff's PII in its system despite the fact that she had not worked there for nearly a decade.

127. Plaintiff Green-Fogg is very careful about sharing her sensitive PII. Ms. Green-Fogg stores any documents containing her PII in a safe and secure location. she has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

128. Plaintiff Green-Fogg received the Notice Letter, by U.S. mail, directly from Defendant, dated June 22, 2023. According to the Notice Letter, Plaintiff's PII was improperly accessed and obtained by unauthorized third parties, including her name, Social Security number, date of birth, bank/financial account information,

routing number, and other information that she may have shared with Defendant in connection with her employment.

129. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Green-Fogg made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: changing passwords and resecuring their own computer systems, filing police reports relating to fraudulent activity, contacting financial institutions to sort out fraudulent activity, pulling credit reports, filing complaints with the FTC, contacting the IRS to secure their accounts, signing up for credit monitoring and identity theft protection, and contacting credit bureaus to place credit alerts on their accounts. Plaintiff Green-Fogg has spent approximately 50 hours thus far dealing with the Data Breach–valuable time Plaintiff Green-Fogg otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

130. Plaintiff Green-Fogg suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to: (a) fraud in the form on a Bank of America account being falsely opened in her name in or about January 2023; (b) out-of-pocket costs spent on LifeLock credit monitoring and identity theft protection services; (c) an increase in spam calls, texts, and/or emails since the Data Breach; (d) invasion of privacy; (e) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity

theft risk; (f) the loss of benefit of the bargain (price premium damages); (g) diminution of value of her PII; and (h) the continued risk to her PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

131. The Data Breach has caused Plaintiff Green-Fogg to suffer fear, anxiety, and stress, which has been compounded by the fact that Citi Trends has still not fully informed him of key details about the Data Breach's occurrence.

132. As a result of the Data Breach, Plaintiff Green-Fogg anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Green-Fogg is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

133. Plaintiff Green-Fogg has a continuing interest in ensuring that her PII, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

134. Plaintiff brings this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

135. The Class that Plaintiff seek to represent is defined as follows:

> All individuals residing in the United States whose PII was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Defendant in June 2023 (the "Class").

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

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

138. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. Upon information and belief, the Data Breach involved thousands of Citi Trends employees and former employees. The Class is apparently identifiable within Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

139. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the

Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

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

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

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

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

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

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

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

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

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

j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;

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

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

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

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

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

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

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

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

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

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

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

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

149. Likewise, particular issues under Rule 42(d)(1) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

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

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

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

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

e. Whether Defendant failed to take commercially reasonable steps to safeguard employee PII; and

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

CAUSES OF ACTION

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

150. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 149 above as if fully set forth herein.

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

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

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

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

155. 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.

156. 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.

157. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

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

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

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

c. Failing to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

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

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

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

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

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

162. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) Plaintiff experiencing fraud in the form on a Bank of America account being falsely opened in her name in or about January 2023; (b) Plaintiff's out-of-pocket costs spent on LifeLock credit monitoring and identity theft protection services; (c) Plaintiff experiencing an increase in spam calls, texts, and/or emails since the Data

Breach; (d) invasion of privacy; (e) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (f) the loss of benefit of the bargain (price premium damages); (g) diminution of value of their PII; and (h) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

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

164. 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
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

165. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 149 above as if fully set forth herein.

166. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

167. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

168. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se.*

169. Plaintiff and Class Members are within the class of persons the statutes were intended to protect and the harm to Plaintiff and Class Members resulting from the Data Breach was the type of harm against which the statutes were intended to prevent.

170. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

171. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendant knew or should have known that they failing to meet its duties, and that Defendants' breach

would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

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

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

173. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 149 above as if fully set forth herein.

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

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

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

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

178. Implicit in the agreement between Plaintiff and Class Members and the Defendant to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, (f) retain the PII only under conditions that kept such information secure and confidential.

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

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

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

182. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

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

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

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

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

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

188. 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 IV
Breach of Implied Covenant of Good Faith and Fair Dealing
(On Behalf of Plaintiff and the Class)

189. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 149 above as if fully set forth herein.

190. Every contract in this State has an implied covenant of good faith and fair dealing. This implied covenant is an independent duty and may be breaches when there is no breach of a contract's actual and/or express terms.

191. Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendant.

192. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard employee PII, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of PII and storage of other personal information after Defendant knew or should have known of the security vulnerabilities of the systems that were exploited in the Data Breach.

193. Defendant acted in bad faith and/or with malicious motive in denying Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT V
Violation of the Georgia Uniform Deceptive Trade Practices Act, Ga. Code Ann. §§ 10-1-370, *et seq.*
(On Behalf of Plaintiff and the Class)

194. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 149 above as if fully set forth herein.

195. Defendant, Plaintiff, and Class Members are "persons" within the meaning of § 10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA").

196. Defendant engaged in deceptive trade practices in the conduct of their business, in violation of Ga. Code § 110-1-372(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another; and

c. Engaging in other conduct that creates a likelihood of confusion or misunderstanding.

197. OSC's and KeyBank's deceptive trade practices include:

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

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

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

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

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

f. Omitting, suppressing, and concealing the material fact that Defendants did not reasonably or adequately secure Plaintiffs' and Class Members' PII; and

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

198. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' Personal Information.

199. Defendant intended to mislead Plaintiff and Class Members and induce them to rely on their misrepresentations and omissions.

200. In the course of its business, Defendant engaged in activities with a tendency or capacity to deceive.

201. Defendant acted intentionally, knowingly, and maliciously to violate Georgia's Uniform Deceptive Trade Practices Act, and recklessly disregarded Plaintiff's and Class Members' rights. Breaches within the financial industry put Defendants on notice that its security and privacy protections were inadequate.

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

203. As a direct and proximate result of Defendant's deceptive trade practices, Plaintiff and Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including loss of the benefit of their bargain with Defendant, as they would not have worked for Defendant or would have demanded to have been paid more for such goods and services but for Defendant's violations alleged herein; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses related to monitoring their financial accounts for fraudulent activity; loss of value of their PII; and an increased, imminent risk of fraud and identity theft.

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

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

205. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 149 above as if fully set forth herein.

206. This count is pleaded in the alternative to Plaintiff's breach of implied contract claim (Count III) and breach of implied covenant of good faith and fair dealing claim (Count IV) above.

207. Plaintiff and Class Members conferred a monetary benefit to Defendant in the form of the provision of their PII and Defendant would be unable to engage in its regular course of business without that PII.

208. Defendant knew that Plaintiff and Class Members conferred a monetary benefit to Defendant and they accepted and retained that benefit. Defendant profited from this monetary benefit, as the transmission of PII to Defendant from Plaintiff and Class Members is an integral part of Defendant's business. Without collecting and maintaining Plaintiff's and Class Members' PII, Defendant would be perform its services.

209. Defendant was supposed to use some of the monetary benefit provided to it by Plaintiff and Class Members to secure the PII belonging to Plaintiff and Class Members by paying for costs of adequate data management and security.

210. Defendant should not be permitted to retain any monetary benefit belonging to Plaintiff and Class Members because Defendant failed to implement necessary security measures to protect the PII of Plaintiff and Class Members.

211. Defendant gained access to the Plaintiff's and Class Members' PII through inequitable means because Defendant failed to disclose that it used inadequate security measures.

212. Plaintiff and Class Members were unaware of the inadequate security measures and would not have entrusted their PII to Defendant had they known of the inadequate security measures.

213. To the extent that this cause of action is pleaded in the alternative to the others, Plaintiff and Class Members have no adequate remedy at law.

214. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (a) Plaintiff experiencing fraud in the form on a Bank of America account being falsely opened in her name in or about January 2023; (b) Plaintiff's out-of-pocket costs spent on LifeLock credit monitoring and identity theft protection services; (c) Plaintiff experiencing an increase in spam calls, texts, and/or emails since the Data Breach;

(d) invasion of privacy; (e) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (f) the loss of benefit of the bargain (price premium damages); (g) diminution of value of their PII; and (h) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

215. 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, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

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

COUNT VII
Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq*
(On Behalf of Plaintiff and the Class)

217. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 149 above as if fully set forth herein.

218. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to

restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this complaint.

219. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and the Class's PII and whether Defendants are currently maintaining data security measures adequate to protect Plaintiff and the Class from further data breaches that compromise their PII. Plaintiff and the Class allege that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Plaintiff and the Class continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future. It is unknown what specific measures and changes Defendant has undertaken in response to the Data Breach.

220. Plaintiff and the Class have an ongoing, actionable dispute arising out of Defendant's inadequate security measures, including (i) Defendant's failure to encrypt Plaintiffs' and the Class's PII, including driver's license numbers, while storing it in an Internet-accessible environment and (ii) Defendant's failure to delete PII it has no reasonable need to maintain in an Internet-accessible environment, including the driver's license number of Plaintiff and the Class.

221. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

222. Defendant owes a legal duty to secure the PII that it continues to maintain;

223. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and

224. Defendant's ongoing breaches of its legal duty continue to cause Plaintiff and the Class harm.

225. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendant to:

a. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

b. audit, test, and train their data security personnel regarding any new or modified procedures and how to respond to a data breach;

c. regularly test its systems for security vulnerabilities, consistent with industry standards; and

d. implement an education and training program for appropriate employees regarding cybersecurity.

226. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data

breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiff and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

227. The hardship to Plaintiff and the Class if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiff and the Class will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

228. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and the Class and others whose confidential information would be further compromised.

COUNT XII
Recovery of Expenses of Litigation, O.C.G.A. § 13-6-11
(On Behalf of Plaintiff and the Class)

229. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 149 above as if fully set forth herein.

230. Pursuant to O.C.G.A. § 13-6-11, the jury may allow the expenses of litigation and attorneys' fees as part of the damages where a defendant "has acted in bad faith, has been stubbornly litigious, or has caused the plaintiff unnecessary trouble and expense."

231. Defendant through its actions alleged and described herein acted in bad faith, were stubbornly litigious, or caused the Plaintiff and the Class Members unnecessary trouble and expense with respect to the transaction or events underlying this litigation.

232. The Plaintiff and the Class Members request that their claim for recovery of expenses of litigation and attorneys' fees be submitted to the jury, and that the Court enter a Judgment awarding their expenses of litigation and attorneys' fees pursuant to O.C.G.A. § 13-6-11.

PRAYER FOR RELIEF

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

A. For an order certifying the Class, as defined herein, and appointing 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 the PII of Plaintiff and Class Members, and from refusing

to issue prompt, complete, any 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 its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws.

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

iv. requiring Defendant to implement and maintain a comprehensive

Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

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

JURY TRIAL DEMANDED

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

Dated: July 14, 2023

Respectfully Submitted,

/s/ Amy C. Daugherty
Amy C. Daugherty
Georgia Bar No. 429299
MaryBeth V. Gibson*
Georgia Bar No. 725843
N. Nickolas Jackson*
Georgia Bar No. 841433
THE FINLEY FIRM, P.C.
3535 Piedmont Road
Building 14, Suite 230
Atlanta, GA 30305
Telephone: (404) 320-9979
Facsimile: (404) 320-9978
adaugherty@thefinleyfirm.com
mgibson@thefinleyfirm.com
njackson@thefinleyfirm.com

David K. Lietz*
MILBERG COLEMAN BRYSON

PHILLIPS GROSSMAN, LLC
5335 Wisconsin Avenue NW
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

Attorneys for Plaintiff and Proposed Class Counsel

**Pro Hac Vice Forthcoming*

ClassAction.org
