

**STATE OF NORTH CAROLINA
COUNTY OF MECKLENBURG**

**IN THE GENERAL COURT OF JUSTICE
SUPERIOR COURT DIVISION
FILE NO: 26CV006404-590**

REECE PAUKEN and JAMAL JOE,
individually and on behalf of all others
similarly situated,

Plaintiff,

v.

AUTOBELL CAR WASH, LLC,

Defendant

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Reece Pauken and Jamal Joe (“Plaintiffs”), individually and on behalf of all others similarly situated, for their Consolidated Class Action Complaint, bring this action against Defendant Autobell Car Wash, LLC (“Defendant” or “Autobell”) based on personal knowledge and the investigation of counsel and alleges as follows:

I. INTRODUCTION

1. Between April 1, 2024 and April 7, 2024, an unknown actor gained access to Defendant’s inadequately protected computer systems. As a result, approximately 52,714 people, including Plaintiffs and the Class Members (as further defined below), have had their personal

identifiable information (“PII”),¹ including their names and Social Security numbers, exposed (the “Data Breach”).²

2. According to Autobell’s website, Autobell is a car wash company with more than 85 locations servicing Delaware, Maryland, North Carolina, South Carolina, and Virginia.³

3. Plaintiffs and the Class Members are current or former employees of Autobell. Autobell employs approximately 3,000 people annually.

4. In carrying out its business, Defendant obtains, collects, uses, and derives a benefit from the PII of Plaintiffs and the Class. As such, Defendant assumed the legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. The Data Breach was discovered on April 7, 2024, when Defendant experienced a security incident that impacted its operations. Autobell hired third-party cybersecurity professionals to investigate the Data Breach.

6. On September 24, 2024, Autobell determined that between April 1, 2024 and April 7, 2024, information stored on Defendant’s network, including Plaintiffs’ and the Class Members’ PII, was accessed and acquired by an unauthorized individual.

7. On October 22, 2024, Defendant began notifying Plaintiffs and Class Members of the Data Breach by mailing them notices of the Data Breach (“Notice Letter”).

¹ Personal identifiable information generally incorporates information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

² OFFICE OF THE MAINE ATTORNEY GENERAL, Data Breach Notifications, <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/c0cef2aa-6844-4cc8-a846-48e88faa4207.html> (last accessed on January 30, 2025).

³ AUTOBELL CAR WASH, *Find an Autobell Location*, <https://www.autobell.com/locations/> (last visited on January 27, 2025).

8. Due to Defendant's negligence, cybercriminals obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals.

9. This class action seeks to redress Defendant's unlawful, willful and wanton failure to protect the personal identifiable information of possibly thousands of individuals that was exposed in a major data breach of Defendant's network in violation of its legal obligations.

10. For the rest of their lives, Plaintiffs and the Class Members will have to deal with the danger of identity thieves possessing and misusing their PII. Plaintiffs and Class Members will have to spend time responding to the Breach and are at an immediate, imminent, and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiffs and Class Members have incurred and/or will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their PII, loss of privacy, and/or additional damages as described below.

11. Defendant betrayed the trust of Plaintiffs and the other Class Members by failing to properly safeguard and protect their PII and thereby enabling cybercriminals to steal such valuable and sensitive information.

12. Plaintiffs bring this action individually and on behalf of the Class, seeking remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, injunctive relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

II. THE PARTIES

13. Plaintiff Reece Pauken is a natural resident of Pineville, North Carolina. Plaintiff Pauken received a Notice Letter from Autobell dated October 22, 2024 informing him that his full name, Social Security number, account number, and routing number were accessed and acquired during the Data Breach.

14. Plaintiff Jamal Joe is a natural resident of High Point, North Carolina. Plaintiff Joe received a Notice Letter from Autobell dated October 22, 2024 informing him that his full name, Social Security number, account number, and routing number were accessed and acquired during the Data Breach.

15. Defendant Autobell is company filed in North Carolina with its principal place of business located in Charlotte, North Carolina.

16. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this Complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

17. All of Plaintiffs' claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

18. This Court has subject matter over this action because this court is a court of original general jurisdiction.

19. Defendant is a citizen of North Carolina because it is filed in North Carolina with its principal place of business in North Carolina.

20. This Court has personal jurisdiction over Defendant because it conducts substantial business in North Carolina and this District and collected and/or stored the PII of Plaintiffs and Class Members in this District.

21. Venue is proper in this District because Defendant operates in this District and a substantial part of the events or omissions giving rise to Plaintiffs and the Class Members' claims occurred in this District, including Defendant collecting and/or storing the PII of Plaintiffs and Class Members.

IV. FACTUAL ALLEGATIONS

Background

22. Defendant is a car wash chain located across Delaware, Maryland, North Carolina, South Carolina, and Virginia with more than 85 locations.⁴

23. Defendant employs approximately 3,000 people annually.

24. In order to gain employment with Defendant, Defendant requires Plaintiffs' and Class Members' PII, including their names, dates of birth, email addresses, physical addresses, Social Security numbers, and financial account information.

25. Defendant collected, stored, and maintained the PII of Plaintiffs and the Class Members on its network. Defendant, however, failed to take reasonable and necessary steps to ensure that its network was secure.

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

⁴ AUTOBELL CAR WASH, *Find an Autobell Location*, <https://www.autobell.com/locations/> (last visited on January 27, 2025).

27. Plaintiffs and the Class Members did not have control over how Defendant stored and maintained their PII. Rather, Plaintiffs were at Defendant's mercy, as Defendant had sole control and authority over its protection of Plaintiffs' and the Class Members' PII.

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

29. Plaintiffs and other Members of the Class entrusted their PII to Defendant.

30. Plaintiffs and Class Members relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use for information for business purposes only, and to only make authorized disclosures of this information. Plaintiffs and Class Members demanded security to safeguard their PII.

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

32. Despite recognizing its duty to do so, on information and belief, Defendant has not implemented reasonable cybersecurity safeguards or policies to protect its consumers' PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. Rather, Defendant chose to store Plaintiffs' and the Class Members' PII on an unsecure network, leaving their PII vulnerable for cybercriminals to take. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to employees' PII.

The Data Breach

33. On or around October 22, 2024, Defendant began sending Plaintiffs and the Class Members notice of the Data Breach, which stated:

What Happened?

On April 7, 2024, Autobell experienced a network security incident that impacted some operations.

What We Are Doing.

Upon learning of this issue, we commenced a prompt investigation working closely with external cybersecurity professionals to determine whether any unauthorized access to protected information. After an extensive forensic investigation and document review, we discovered on September 24, 2024, that between April 1, 2024 and April 7, 2024, certain information stored on our network may have been accessed and/or acquired by an unauthorized individual.

What Information Was Involved?

The impacted information includes your full name and the following: Social Security number, account number, and routing number.

Notice Letter, attached as Exhibits 1 & 2.

34. Omitted from the Notice Letter were the identity of the cybercriminals who perpetrated this Data Breach, the date that Defendant detected 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 Plaintiffs 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, Plaintiffs and Class Members of the Data Breach’s critical facts. Without these details, Plaintiffs’ and Class Members’ ability to mitigate the harms resulting from the Data Breach is severely diminished.

36. Despite Defendant’s intentional opacity about the root cause of this incident, several facts may be gleaned from the Notice Letter, including: a) that this Data Breach was the work of cybercriminals; b) that the cybercriminals first infiltrated Defendant’s networks and

systems, and downloaded data from the networks and systems (aka exfiltrated data, or in layperson's terms "stole" data; and c) that once inside Defendant's networks and systems, the cybercriminals targeted information including Plaintiffs' and Class Members' Social Security numbers for download and theft.

37. Moreover, in its Notice Letter, Defendant failed to specify whether it undertook any efforts to contact the Class Members whose data was accessed and acquired in the Data Breach to inquire whether any of the Class Members suffered misuse of their data, whether Class Members should report their misuse to Defendant, and whether Defendant set up any mechanism for Class Members to report any misuse of their data.

38. Notably, according to Defendant's own admission, Defendant's network failed to detect the Data Breach and notify Defendant of the Data Breach until days later when the damage had already been done.

39. The targeted cyberattack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the PII of employees like Plaintiffs and Class Members.

40. The unencrypted PII of Plaintiffs and Class Members may end up or already has ended up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

41. Defendant was negligent and did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiffs and Class Members, causing the exposure of PII for Plaintiffs and Class Members.

42. Because Defendant had a duty to protect Plaintiffs' and Class Members' PII, Defendant should have known through readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

43. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;
- b. Failing to adequately protect employees' PII;
- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;
- e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;
- f. Failing to ensure the confidentiality and integrity of electronic PII it created, received, maintained, and/or transmitted;
- g. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PII to allow access only to those persons or software programs that have been granted access rights;
- h. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations;

- i. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports;
- j. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PII;
- k. Failing to protect against reasonably anticipated uses or disclosures of electronic PII that are not permitted under the privacy rules;
- l. Failing to train all members of its workforces effectively on the policies and procedures regarding PII as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PII;
- m. Failing to render the electronic PII it maintained unusable, unreadable, or indecipherable to unauthorized individuals, as it had not encrypted the electronic PII;
- n. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;
- o. Failing to adhere to industry standards for cybersecurity; and
- p. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

44. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' PII by allowing cyberthieves to access Defendant's computer network and systems which contained unsecured and unencrypted PII.

45. Accordingly, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and the Class Members also lost the benefit of the bargain they made with Defendant.

The Data Breach was Foreseeable

46. Because Defendant had a duty to protect Plaintiffs' and Class Members' PII, Defendant should have known through readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

47. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks because warnings were readily available and accessible via the internet.

48. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."⁵

49. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize

⁵ FBI, High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations (Oct. 2, 2019) (emphasis added), *available at* <https://www.ic3.gov/Media/Y2019/PSA191002> (last visited Jan. 25, 2022).

damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay.”⁶

50. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a “Ransomware Guide” advising that “[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion.”⁷

51. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that: (i) cybercriminals were targeting big companies such as Defendant, (ii) cybercriminals were ferociously aggressive in their pursuit of companies in possession of significant sensitive information such as Defendant, (iii) cybercriminals were leaking corporate information on dark web portals, and (iv) cybercriminals’ tactics included threatening to release stolen data.

52. Moreover, Defendant knew or should have known of the risks because employers in possession of PII are particularly susceptible to cyber-attacks.

53. 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.

⁶ ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), available at <https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/> (last visited Jan. 25, 2022).

⁷ U.S. CISA, Ransomware Guide – September 2020, available at https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf (last visited Jan. 25, 2022).

54. 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.

55. In 2023, an all-time high for data compromises occurred, with 3,205 compromises affecting 353,027,892 total victims.⁸ Of the 3,205 recorded data compromises, 809 of them, or 25.2% were in the medical or healthcare industry.⁹ The estimated number of organizations impacted by data compromises has increased by +2,600 percentage points since 2018, and the estimated number of victims has increased by +1400 percentage points.¹⁰ The 2023 compromises represent a 78 percentage point increase over the previous year and a 72 percentage point hike from the previous all-time high number of compromises (1,860) set in 2021.¹¹

56. In light of recent high profile data breaches at other industry leading companies, including T-Mobile, USA (37 million records, February-March 2023), 23andMe, Inc. (20 million records, October 2023), Wilton Reassurance Company (1.4 million records, June 2023), NCB Management Services, Inc. (1 million records, February 2023), Defendant knew or should have known that the PII that it collected and maintained would be targeted by cybercriminals.

57. Additionally, as companies became more dependent on computer systems to run their business,¹² 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

⁸ 2023 Data Breach Annual Report, IDENTITY THEFT RESOURCE CENTER (Jan. 2024) https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf.

⁹ *Id.*

¹⁰ *Id.*

¹¹ *Id.*

¹² Danny Brando, et al., BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, FEDS Notes, *Implications of Cyber Risk for Financial Stability* (May 12, 2022)

for adequate administrative, physical, and technical safeguards.¹³

58. Considering the information readily available and accessible on the internet before the Data Breach and Defendant's status as an employer, Defendant, having elected to store the unencrypted PII of Plaintiffs and Class Members in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII, and Defendant's type of business had cause to be particularly on guard against such an attack.

59. Prior to the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack.

60. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted or destroyed the Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

The Data Breach was Preventable

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

62. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."¹⁴

<https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>.

¹³ Dr. Suleyman Ozarslan, PICUS, *Key Threats and Cyber Risks Facing Financial Services and Banking Firms in 2022* (Mar. 24, 2022) <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022>.

¹⁴ 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 July 17, 2023).

63. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

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

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.¹⁵

64. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks. . . .
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net). . . .
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it. . . .
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You

¹⁵ *Id.* at 3-4.

may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic. . . .¹⁶

65. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; Remove privilege credentials

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise

Include IT Pros in security discussions

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

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- Apply principle of least-privilege

Monitor for adversarial activities

- Hunt for brute force attempts
- Monitor for cleanup of Event logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection

¹⁶ See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* <https://www.cisa.gov/news-events/news/protecting-against-ransomware> (last visited July 17, 2023).

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].¹⁷

66. Given that Defendant was storing the PII of other individuals, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

67. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of Plaintiffs and Class Members.

68. Defendant could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing the PII of Plaintiffs and Class Members. Alternatively, Defendant could have destroyed the data it no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

69. Defendant's negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

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

71. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable,

¹⁷ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited July 17, 2023).

required, and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the Plaintiffs' and Class Members' PII was compromised through disclosure to an unknown and unauthorized criminal third party.

72. Upon information and belief, Defendant breached its duties and obligations in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiffs and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the PII; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack; and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents

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

Defendant Failed to Adhere to FTC Guidelines

74. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

75. The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”¹⁸ 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.”¹⁹

76. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

- a. Protect the sensitive consumer information that they keep;
- b. Properly dispose of PII that is no longer needed;
- c. Encrypt information stored on computer networks;
- d. Understand their network’s vulnerabilities; and
- e. Implement policies to correct security problems.

77. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

78. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity

¹⁸ 17 C.F.R. § 248.201 (2013).

¹⁹ *Id.*

on the network; and verify that third-party service providers have implemented reasonable security measures.

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

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

Defendant Fails to Comply with Industry Standards

81. As shown above, experts studying cybersecurity routinely identify healthcare providers and partners as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

82. Several best practices have been identified that at a minimum should be implemented by healthcare providers 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.

83. Other best cybersecurity practices that are standard in the healthcare industry 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.

84. 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.

85. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

Defendant's Response to the Data Breach is Inadequate

86. Defendant was negligent and failed to inform Plaintiffs and the Class Members of the Data Breach in time for them to protect themselves from identity theft.

87. Defendant admitted that it learned of the data breach on April 7, 2024. Yet, Defendant did not conclude its investigation into the Data Breach until months later on September 24, 2024.

88. Defendant further delayed notifying affected individuals and did not send out notices until late October 2024.

89. During these intervals, the cybercriminals have had the opportunity to exploit the Plaintiffs and the Class Member's PII while Defendant was secretly investigating the Data Breach.

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

91. To date, Defendant has offered Plaintiffs and some Class Members only twelve (12) months of credit monitoring services. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' PII. Moreover, once this service expires, Plaintiffs and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

Value of PII

92. 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. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.²⁰ Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.²¹ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.²²

²⁰ *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 accessed July 17, 2023).

²¹ *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 accessed July 17, 2023).

²² *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed July 17, 2023).

93. 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.

94. 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.”²³

95. 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.

96. One such example of criminals using PII for profit is the development of “Fullz” packages.

97. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as “Fullz” packages.

98. The development of “Fullz” packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs’ and the Class’s phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain

²³ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed July 17, 2023).

information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

99. Of course, a stolen Social Security number – standing alone – can be used to wreak untold havoc upon a victim’s personal and financial life. The popular person privacy and credit monitoring service LifeLock by Norton notes “Five Malicious Ways a Thief Can Use Your Social Security Number,” including 1) Financial Identity Theft that includes “false applications for loans, credit cards or bank accounts in your name or withdraw money from your accounts, and which can encompass credit card fraud, bank fraud, computer fraud, wire fraud, mail fraud and employment fraud; 2) Government Identity Theft, including tax refund fraud; 3) Criminal Identity Theft, which involves using someone’s stolen Social Security number as a “get out of jail free card;” 4) Medical Identity Theft, and 5) Utility Fraud.²⁴

100. That is exactly what is happening to Plaintiffs and members of the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs’ and the Class’s stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

Plaintiffs’ Injuries and Experiences

A. Plaintiff Pauken

101. Plaintiff Pauken entrusted his PII to Defendant. Defendant required Plaintiff Pauken’s PII – including his name, Social Security number, driver’s license number, address,

²⁴ *Alison Grace Johansen, LIFELOCK BY NORTON, 5 Kinds of ID Theft Using a Social Security Number* (Nov. 30, 2017) https://lifelock.norton.com/learn/identity-theft-resources/kinds-of-id-theft-using-social-security-number?srltid=AfmBOooE5NTQZXogBjQqTWSCLi-jDIeZlZGt2jjOGslBjhZuR_rwOTJN.

email, phone number, and financial account information – in order to gain employment with Defendant.

102. Plaintiff Pauken worked for Defendant up until 2022.

103. Plaintiff Joe received a Notice of the Data Breach dated October 22, 2024, informing him that his PII, including his name, Social Security number, account number, and routing number were impacted by the Data Breach.

104. After the Data Breach, Plaintiff Pauken began receiving an increased amount of spam phone calls and emails.

105. As a result of the Data Breach, Plaintiff Pauken's sensitive information may have been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Pauken's sensitive information has been irreparably harmed. For the rest of his life, Plaintiff Pauken will have to worry about when and how his sensitive information may be shared or used to his detriment

106. As a result of the Data Breach, Plaintiff Pauken spent time dealing with the consequences of the Data Breach, which includes times spent verifying the legitimacy of the Notice Letter and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

107. Additionally, Plaintiff Pauken is very careful about not sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

108. Plaintiff Pauken stores any documents containing his sensitive PII in safe and secure locations or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

109. Plaintiff Pauken suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and experiences fear and anxiety and increased concern for the loss of his privacy.

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

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

B. Plaintiff Joe

112. Plaintiff Joe entrusted his PII to Defendant. Defendant required Plaintiff Joe's PII – including his name, Social Security number, driver's license number, address, email, phone number, and financial account information – in order to gain employment with Defendant.

113. Plaintiff Joe worked for Defendant in 2023.

114. Plaintiff Joe received a Notice of the Data Breach dated October 22, 2024, informing him that his PII, including his name, Social Security number, account number, and routing number were impacted by the Data Breach.

115. After the Data Breach, Plaintiff Joe began receiving an increased amount of spam phone calls and emails. Prior to the Data Breach, Plaintiff Joe did not receive this level of spam calls and emails.

116. After the Data Breach, in 2024, Plaintiff Joe tried to go to Verizon to get a new cell phone, but his credit was denied. He has not used this line of credit and has no unpaid bills. Yet,

Verizon represented to him that he cannot use his line of credit. Plaintiff Joe reasonably believes that the Data Breach has impacted his ability to use his credit. Plaintiff Joe has requested his credit report statements and is waiting to receive those statements in the mail.

117. Using someone's credit is the quintessential example of damages resulting from having one's PII exposed. Armed with a victim's name and Social Security number, cybercriminals are able to pose as the victim and take out loans or run up a credit bill, all without the victim's knowledge.

118. As a result of the Data Breach, Plaintiff Joe's sensitive information may have been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Joe's sensitive information has been irreparably harmed. For the rest of his life, Plaintiff Joe will have to worry about when and how his sensitive information may be shared or used to his detriment

119. As a result of the Data Breach, Plaintiff Joe spent time dealing with the consequences of the Data Breach, which includes times spent verifying the legitimacy of the Notice Letter and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

120. Additionally, Plaintiff Joe is very careful about not sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

121. Plaintiff Joe stores any documents containing his sensitive PII in safe and secure locations or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

122. Plaintiff Joe suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and experiences fear and anxiety and increased concern for the loss of his privacy.

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

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

Plaintiffs and the Class Members Damages and Injuries

125. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

126. Defendant negligently disclosed the PII of Plaintiffs and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiffs and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

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

128. Defendant was, or should have been, fully aware of the unique type and the significant volume of data contained in Defendant's database, 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.

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

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

131. As a result of Defendant's negligence and failure to prevent the Data Breach, Plaintiffs and the Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

- a. Identity theft;
- b. Misuse of their PII;
- c. The loss of the opportunity to control how their PII is used;
- d. The diminution in value of their PII;
- e. The compromise and continuing publication of their PII;
- f. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

- g. Loss opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spend researching how to prevent, detect, contest, and recover form identity theft and fraud;
- h. Nominal damages;
- i. Lost benefit of the bargain;
- j. Invasion of privacy;
- k. Delay in receipt of tax refund monies;
- l. Unauthorized use of stolen PII; and
- m. The continued risk to their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in their possession.

Plaintiffs' and the Class Members' PII is Available on the Dark Web

132. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiffs' and Class Members' PII with the intent of engaging in misuse of the PII, including marketing and selling Plaintiffs' and Class Members' PII.

133. Upon information and believe, the unencrypted Private Information of Plaintiffs and Class Members is for sale on the dark web because that is the *modus operandi* of hackers.

134. The targeted cyberattack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the PII of employees like Plaintiffs and Class Members.

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

136. Plaintiffs have already seen identity theft and fraud. Plaintiffs did not have any issues with this prior to the Data Breach. As such, Plaintiffs have further reason to believe that their information, and the Class's information, was sold on the Dark Web, resulting in the fraudulent misuse.

137. The dark web is an unindexed layer of the internet that requires special software or authentication to access.²⁵ Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or "surface" web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.²⁶ This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

138. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, PII like the Private Information at issue here.²⁷ The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen

²⁵ *What Is the dark web?*, Experian, available at <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/>.

²⁶ *Id.*

²⁷ *What is the dark web?* – Microsoft 365, available at <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web>.

financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.²⁸ As Microsoft warns “[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others.”²⁹

Plaintiffs and the Class Members Have Experienced Misuse of Their PII

139. As a result of the Data Breach, the unencrypted and detailed PII of Plaintiffs and the Class Members has fallen into the hands of companies that will use it for targeted marketing without the approval of Plaintiffs and Class Members, as seen by the increase in spam calls and emails. Unauthorized actors can easily access and misuse Plaintiffs’ and Class Members’ PII due to the Data Breach. Plaintiffs have already experienced misuse of their PII as a result of the Data Breach.

140. 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 herein.

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

142. For example, armed with just a name and Social Security number, a data thief can utilize a hacking technique referred to as “social engineering” to obtain even more information

²⁸ *Id.*; *What Is the dark web?*, Experian, available at <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/>.

²⁹ *What is the dark web?* – Microsoft 365, available at <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web>.

about a victim's identity, such as a person's login credentials or financial account information. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

143. Moreover, the existence and prevalence of “Fullz” packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

144. 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.

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

146. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not 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.^[30]

³⁰ Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

147. 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.

148. Even then, new Social Security number may not be effective, as “[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”³¹

149. For these reasons, some courts have referred to Social Security numbers as the “gold standard” for identity theft. *Portier v. NEO Tech. Sols.*, No. 3:17-CV-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) (“Because Social Security numbers are the gold standard for identity theft, their theft is significant Access to Social Security numbers causes long lasting jeopardy because the Social Security Administration does not normally replace Social Security numbers.”), report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc.*, 2021 WL 860584, at *4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiff’s Social Security numbers are: arguably “the most dangerous type of personal information in the hands of identity thieves” because it is immutable and can be used to “impersonat[e] [the victim] to get medical services, government benefits, . . . tax refunds, [and] employment.” . . . Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, “[a] social security number derives its value in that it is immutable,” and when it is stolen it can “forever be wielded to identify

³¹ Brian Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last visited Aug. 23, 2024).

[the victim] and target his in fraudulent schemes and identity theft attacks.”).

150. Similarly, the California state government warns consumers that: “[o]riginally, your Social Security number (SSN) was a way for the government to track your earning and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information. With your name and SSN, an identity thief could open a new credit and bank account, rent an apartment, or even get a job.”³²

151. Identity thieves can also use Social Security numbers to obtain a driver’s license or official identification card in the victim’s name but with the thief’s picture; use the victim’s name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim’s information. In addition, identity thieves may obtain a job using the victim’s Social Security number, rent a house or receive medical services in the victim’s name, and may even give the victim’s personal information to police during an arrest resulting in an arrest warrant issued in the victim’s name. And the Social Security Administration has warned that identity thieves can use an individual’s Social Security number to apply for credit lines.³³

152. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice,

A direct financial loss is the monetary amount the offender obtained from misusing the victim’s account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect

³² *Your Social Security Number: Controlling the Key to Identity Theft*, Rob Bonta Attorney General, <https://oag.ca.gov/idtheft/facts/your-ssn> (last accessed on January 21, 2024).

³³ *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2018), available at <https://www.ssa.gov/pubs/EN-05-10064.pdf>.

losses are included in the calculation of out-of-pocket loss.^[34]

153. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than \$3.5 billion in losses to individuals and business victims.³⁵

154. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."³⁶ Yet, Defendants failed to rapidly report to Plaintiffs and Class Members that their Private Information was stolen.

Plaintiffs' and the Class Members' Lost Time

155. Plaintiffs and the Class Members have also spent considerable time and will continue to spend considerable time to protect themselves and keep their identities and personal property protected, including researching and verifying the legitimacy of the Data Breach, changing passwords and resecuring their own computer networks, and contacting credit bureaus to place freezes on their accounts. Accordingly, the Data Breach has caused Plaintiffs and Class Members to suffer actual injury in the form of lost time—which cannot be recaptured – spent on mitigation activities.

156. 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.

³⁴ Erika Harrell, *Bureau of Just. Stat.*, U.S. DEP'T OF JUST., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) <https://bjs.ojp.gov/content/pub/pdf/vit18.pdf> (last accessed Jan. 23, 2024).

³⁵ See <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120>.

³⁶ *Id.*

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.

157. Thus, due to the actual and imminent risk of identity theft, Defendant, in its Notice Letter instructs Plaintiffs and Class Members to take the following measures to protect themselves: “remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.” Exs. 1 & 2.

158. In addition, Defendant’s Notice letter includes multiple pages devoted to “Other Important Information” that recommend Plaintiffs and Class Members to partake in activities such as monitoring their accounts, placing fraud alerts on their accounts, and contacting consumer reporting bureaus. *Id.*

159. Defendant’s extensive suggestion of steps that Plaintiffs and Class Members must take in order to protect themselves from identity theft and/or fraud demonstrates the significant time that Plaintiffs and Class Members must undertake in response to the Data Breach. Plaintiffs’ and Class Members’ time is highly valuable and irreplaceable, and accordingly, Plaintiffs and Class Members suffered actual injury and damages in the form of lost time that they spent on mitigation activities in response to the Data Breach and at the direction of Defendant’s Notice Letter.

160. Plaintiffs’ 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.”³⁷

³⁷ 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>.

161. Plaintiffs’ mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.³⁸

162. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”³⁹

163. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.⁴⁰

164. According to the U.S. Bureau of Labor Statistics’ 2018 American Time Use Survey, American adults have only 36 to 40 hours of “leisure time” outside of work per week; leisure time is defined as time not occupied with work or chores and is “the time equivalent of ‘disposable

³⁸ Federal Trade Commission, Identity Theft.gov, <https://www.identitytheft.gov/Steps> (last visited July 7, 2022).

³⁹ “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”).

⁴⁰ *Characteristics of Minimum Wage Workers, 2020*, U.S. BUREAU OF LABOR STATISTICS <https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=%20In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour> (last accessed March 18, 2024); *Average Weekly Wage Data*, U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data*, <https://www.bls.gov/news.release/pdf/wkyeng.pdf> (last accessed May 9 2024) (finding that on average, private-sector workers make \$1,145 per 40-hour work week.).

income.”⁴¹ Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

165. Plaintiffs and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek remuneration for the loss of valuable time as another element of damages.

Plaintiffs’ and the Class Members Heightened Risk of Identity Theft and Ongoing Injuries

166. Cyberattacks and data breaches at employers like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

167. The United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft face “substantial costs and time to repair the damage to their good name and credit record.”⁴²

168. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims’ identities in order to engage in illegal financial transactions under the victims’ names. Because a person’s identity is

⁴¹ Cory Stieg, *You’re spending your free time wrong — here’s what to do to be happier and more successful*, CNBC <https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html> (Nov. 6, 2019) (last accessed May 9, 2024).

⁴² U.S. Gov’t Accounting Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (2007), available at <https://www.gao.gov/new.items/d07737.pdf> (last visited March 18, 2024).

akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

169. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.⁴³

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

171. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give

⁴³ *IdentityTheft.gov*, Federal Trade Commission, <https://www.identitytheft.gov/Steps> (last visited March 18, 2024).

the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

172. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.⁴⁴

173. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that 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.

174. Additional fraudulent activity resulting from the Data Breach may not come to light for years.

175. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.⁴⁵

176. As a result of the Data Breach, Cybercriminals also have sufficient information to pose as legitimate persons and gain more information from Plaintiffs and the Class Members, putting Plaintiffs and the Class Members at a continuing risk of identity theft.

177. Victims of identity theft also often suffer embarrassment, blackmail, or harassment

⁴⁴ 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).

⁴⁵ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last accessed July 17, 2023).

in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

178. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

179. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiffs and Class Members will need to remain vigilant for years or even decades to come.

180. Defendant's negligence and failure to properly notify Plaintiffs and members of the Class of the Data Breach exacerbated Plaintiffs' and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

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

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

182. To date, Defendant has offered Plaintiffs and some Class Members an inadequate amount of credit monitoring services. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

183. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII, and the *modus operandi* of cybercriminals, 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, filing false tax returns, taking out loans or lines of credit, or filing false unemployment claims.

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

185. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.⁴⁶ The information disclosed in this Data Breach is impossible to “close” and difficult, if not impossible, to change (such as Social Security numbers).

186. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future, if not forever.

187. The retail cost of credit monitoring and identity theft monitoring can cost \$200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant’s Data Breach. This is a future cost for a

⁴⁶ See Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1>.

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

Diminution of Value of PII

188. PII is a valuable property right.⁴⁷

189. 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.

190. Sensitive PII can sell for as much as \$363 per record according to the Infosec Institute.⁴⁸

191. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly \$200 billion.⁴⁹ In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.⁵⁰

⁴⁷ "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").

⁴⁸ 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).

⁴⁹ 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).

⁵⁰ David Lazarus, *Column: Shadow Data Brokers Make the Most of Their Invisibility Cloak*, LOS ANGELES TIMES (Nov. 5, 2019) <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>.

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

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

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

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

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

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

Loss Benefit of the Bargain

198. Further, Defendant's poor data security deprived Plaintiffs and the Class Members of the benefit of the bargain.

199. When agreeing to obtain employment with Defendant under certain terms, Plaintiffs and the other reasonable employees understood and expected that Defendant would properly safeguard and protect their PII.

200. However, Defendant did not provide the expected data security.

201. Accordingly, Plaintiffs and the Class Members received employment positions of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

V. CLASS ACTION ALLEGATIONS

202. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23 of the North Carolina Rules of Civil Procedure.

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

All individuals whose PII may have been accessed and/or acquired in the ransomware attack that is the subject of the Notice Letters that Defendant sent to Plaintiffs and Class Members on or around October 22, 2024 (the "Class").

204. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

205. Plaintiffs reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

206. **Numerosity:** The Class is so numerous that joinder of all members is impracticable. Defendant reported to the Maine Attorney General at approximately 52,714 people were involved in the Data Breach.⁵¹

207. **Commonality:** Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiffs and Class Members;
- b. Whether Defendant had duties not to disclose the PII of Plaintiffs and Class Members to unauthorized third parties;
- c. Whether Defendant had duties not to use the PII of Plaintiffs and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class Members;
- e. Whether Defendant failed to timely destroy the PII of Plaintiffs and the Class Members;
- f. When Defendant actually learned of the Data Breach;
- g. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;
- h. Whether Defendant violated the law by failing to promptly notify Plaintiffs

⁵¹ OFFICE OF THE MAINE ATTORNEY GENERAL, Data Breach Notifications, <https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/c0cef2aa-6844-4cc8-a846-48e88faa4207.html> (last accessed on January 30, 2025).

and Class Members that their PII had been compromised;

i. 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;

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

k. Whether Defendant engaged in unfair, unlawful, or deceptive practice by failing to safeguard the PII of Plaintiffs and Class Members;

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

m. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

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

208. **Typicality:** Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

209. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendant has 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 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 Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

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

211. **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.

212. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the

costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

213. 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.

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

215. 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.

216. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to Class Members as a whole is appropriate under Rule 23 of the North Carolina Rules of Civil Procedure.

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

- a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
- b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, safeguarding, and failing to destroy their PII;
- c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their PII had been compromised;
- e. 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;
- f. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members; and,
- g. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

VI. CAUSES OF ACTION

COUNT I – NEGLIGENCE **(On Behalf of Plaintiffs and the Class)**

218. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

219. Defendant solicited, gathered, and stored the PII Plaintiffs and the Class as part of the operation of its business.

220. Upon accepting and storing the PII of Plaintiffs and Class Members, Defendant undertook and owed a duty to Plaintiffs and Class Members to exercise reasonable care to secure and safeguard that information and to use secure methods to do so.

221. Defendant had full knowledge of the sensitivity of the PII, the types of harm that Plaintiffs and Class members could and would suffer if the PII was wrongfully disclosed, and the importance of adequate security.

222. Plaintiffs and Class members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class members had no ability to protect their PII that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiffs and the Class.

223. Defendant was well aware of the fact that cyber criminals routinely target large corporations through cyberattacks in an attempt to steal sensitive PII.

224. Defendant owed Plaintiffs and the Class members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data.

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

226. Defendant had duties to protect and safeguard the PII of Plaintiffs and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive PII. Additional duties that Defendant owed Plaintiffs and the Class include:

- a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class Members' PII was adequately secured from impermissible access, viewing, release, disclosure, and publication;
- b. To protect Plaintiffs' and Class Members' PII in its possession by using reasonable and adequate security procedures and systems;
- c. To implement processes to quickly detect a data breach, security incident, or intrusion involving their networks and servers; and
- d. To promptly notify Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

227. Defendant was the only one who could ensure that its systems and protocols were sufficient to protect the PII that Plaintiffs and the Class had entrusted to it.

228. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and Class Members' PII. Defendant breached its duties by, among other things:

- a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the PII in its possession;
- b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;

- c. Failing to adequately train its employees to not store PII longer than absolutely necessary;
- d. Failing to consistently enforce security policies aimed at protecting Plaintiffs' and the Class's PII; and
- e. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions.

229. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

230. As a proximate and foreseeable result of Defendant's negligent and/or grossly negligent conduct, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages.

231. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the PII of Plaintiffs and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiffs and Class Members while it was within Defendant's possession and control.

232. As a result of the Data Breach, Plaintiffs and Class Members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, closely reviewing and monitoring bank accounts, credit reports, and statements sent from providers and their insurance companies and the payment for credit monitoring and identity theft prevention services.

233. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

234. The damages Plaintiffs and the Class have suffered and will suffer were and are the direct and proximate result of Defendant's negligent and/or grossly negligent conduct.

COUNT II – NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)

235. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

236. In addition to its duties under common law, Defendant had additional duties imposed by statute and regulations, including the duties the FTC Act. The harms which occurred as a result of Defendant's failure to observe these duties, including the loss of privacy and significant risk of identity theft, are the types of harm that these statutes and their regulations were intended to prevent.

237. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' PII.

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

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

240. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se* as Defendant's violation of the FTC Act establishes the duty and breach elements of negligence.

241. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

242. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

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

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

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

COUNT III – BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

246. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

247. Plaintiffs and Class Members were required to provide their PII to Defendant as a condition of receiving employment provided by Defendant. Plaintiffs and Class Members provided their PII to Defendant or its third-party agents in exchange for Defendant's employment.

248. Plaintiffs and Class Members reasonably understood that a portion of the funds derived from their employment would be used to pay for adequate cybersecurity measures. Plaintiffs and Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

249. Plaintiffs and the Class Members accepted Defendant's offers by disclosing their PII to Defendant or its third-party agents in exchange for employment.

250. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII to unauthorized persons.

251. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiffs' and Class Member's PII.

252. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and Class members with prompt and adequate notice of all unauthorized access and/or theft of their PII.

253. After all, Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

254. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

255. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain.

256. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

257. Defendant materially breached the contracts it entered with Plaintiffs and Class Members by:

- a. failing to safeguard their information;
- b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.
- c. failing to comply with industry standards;
- d. failing to comply with the legal obligations necessarily incorporated into the agreements; and
- e. failing to ensure the confidentiality and integrity of the electronic PII that Defendant created, received, maintained, and transmitted.

258. In these and other ways, Defendant violated its duty of good faith and fair dealing.

259. Defendant's material breaches were the direct and proximate cause of Plaintiffs' and Class Members' injuries (as detailed *supra*).

260. And, on information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

261. Plaintiffs and Class Members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

COUNT IV – UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

262. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

263. Plaintiffs and Class Members conferred a benefit upon Defendant. After all, Defendant benefitted from using their employment and PII to derive profit and facilitate its business.

264. Defendant appreciated or had knowledge of the benefits it received from Plaintiffs and Class Members.

265. Plaintiffs and Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

266. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII.

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

268. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and Class Members' employment and PII because Defendant failed to adequately protect their PII.

269. Plaintiffs and Class Members have no adequate remedy at law.

270. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiffs and Class Members—all unlawful or inequitable proceeds that it received because of its misconduct.

**COUNT V – VIOLATION OF THE NORTH CAROLINA DECEPTIVE
AND UNFAIR TRADE PRACTICES ACT, N.C. GEN. STAT. § 75-1.1**
(On Behalf of Plaintiffs and the Class)

271. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

272. Under N.C. Gen. Stat. § 75-1.1, “[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are declared unlawful.”

273. Defendant is subject to N.C. Gen. Stat. § 75-1.1, because Defendant engages in commerce in North Carolina. After all, Defendant engages in “business activities” within North Carolina.

274. Defendant violated N.C. Gen. Stat. § 75-1.1 by, inter alia:

- a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs’ 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 Plaintiffs’ and Class members’ PII, including duties

imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*, which was a direct and proximate cause of the Data Breach;

- d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' PII; and
- e. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA, 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

275. Defendant's 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 their PII.

276. Defendant intended to mislead Plaintiffs and Class members and induce them to rely on its omissions.

277. 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. Defendant accepted the PII that Plaintiffs and Class members entrusted to it while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiffs and Class members acted reasonably in relying on Defendant's omissions, the truth of which they could not have discovered through reasonable investigation.

278. Defendant acted intentionally, knowingly, maliciously, and recklessly disregarded

Plaintiffs' and Class members' rights.

279. As a direct and proximate result of Defendant's unfair and deceptive acts and practices, Plaintiffs and Class members have suffered and will continue to suffer injury ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII.

280. And, on information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

281. Plaintiffs and Class members seek all monetary and non-monetary relief allowed by law.

COUNT VI – DECLARTORY JUDGMENT
(On Behalf of Plaintiffs and the Class)

282. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

283. 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.

284. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and the Class's PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and the Class from further data breaches that compromise their PII. Plaintiffs alleges that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Plaintiffs continues to suffer injury as a result of the

compromise of her PII and remains 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.

285. Plaintiffs 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 Social Security 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 Social Security numbers of Plaintiffs and the Class.

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

- a. Defendant owes a legal duty to secure the PII of Plaintiffs and the Class;
- b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and
- c. Defendant's ongoing breaches of its legal duty continue to cause Plaintiffs and the Class harm.

287. 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 its 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;
- d. implement an education and training program for appropriate employees regarding cybersecurity.

288. If an injunction is not issued, Plaintiffs and Class Members 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, Plaintiffs 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.

289. The hardship to Plaintiffs and Class Members if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiffs 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.

290. 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 Plaintiffs and others whose confidential information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for judgment against Defendant as follows:

- a. An order certifying this action as a class action under N.C. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class

counsel, and finding that Plaintiffs are a proper representative of the Class requested herein;

- b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including actual and statutory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;
- c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the general public as requested herein, including, but not limited to:
 - i. Ordering that Defendant engage 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;
 - ii. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
 - iii. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;
 - iv. Ordering that Defendant segment employee data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

- v. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner employee data not necessary for their provisions of services;
 - vi. Ordering that Defendant conduct regular database scanning and securing checks; and
 - vii. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.
- d. An order requiring Defendant to pay the costs involved in notifying the Class members about the judgment and administering the claims process;
 - e. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and
 - f. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable.

Dated: February 2, 2026

Respectfully submitted,

/s/ Nevin Wisnoski
Nevin Wisnoski (NC Bar #55038)
MILBERG, PLLC
800 S. Gay Street, Suite 1100
Knoxville, TN 37929
Telephone: (919) 585-4630
nwisnoski@milberg.com

Jessica A. Wilkes (*pro hac vice* forthcoming)
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, OK 73120
Telephone: (405) 235-1560
jaw@federmanlaw.com

Counsel for Plaintiffs and Proposed Class