FILED
2024 Jul-30 PM 05:06
U.S. DISTRICT COURT
N.D. OF ALABAMA

THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ALABAMA

MICHAEL HARRISON, ALLAN CARSON, ARTHUR HUGHES, CRYSTAL HARGRAVE, and KRISTI FEYJES on behalf of themselves and all others similarly situated **Plaintiffs,** **v.** **PECO FOODS, INC.,** **Defendant.**	**Case No.:** **COMPLAINT-CLASS ACTION** **DEMAND FOR JURY TRIAL**

Plaintiffs Michael Harrison, Allan Carson, Arthur Hughes, Crystal Hargrave, and Kristi Feyjes (collectively "Plaintiffs") bring this Class Action Complaint against Peco Foods, Inc. ("Peco" or "Defendant"), individually and on behalf of all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard personal identifiable information ("PII")[1] of at least 48,170 individuals,[2] including, on information and belief such personal information an employer keeps for their employees, such as name, date of birth, federal/state identification numbers, social security number, financial information and/or other information such as phone number, address, and email address.

2. Peco Foods is the 8th largest poultry producer in the United States and a fully

[1] Personally 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..

[2] https://www.comparitech.com/news/poultry-processor-peco-foods-notifies-48k-people-of-data-breach-offers-free-credit-monitoring/ (last viewed July 29, 2024).

integrated grower, processor and marketer. Their corporate offices are located in Tuscaloosa, Alabama.[3] Peco employs individuals at its plants and corporate offices in Alabama, Arkansas and Mississippi.

3. Prior to and through December 4, 2023, Defendant obtained the PII of Plaintiffs and Class Members, including by collecting it directly from Plaintiffs and Class Members.

4. Prior to and through December 4, 2023, Defendant stored the PII of Plaintiffs and Class Members, unencrypted, in an Internet-accessible environment on Defendant's network.

5. On or before May 23, 2023, Defendant learned of a data breach on its network that occurred on or around December 4, 2023 (the "Data Breach").

6. Defendant determined that, during the Data Breach, a ransomware gang accessed and/or acquired the PII of Plaintiffs and Class Members. On information and belief, a ransomware gang has claimed responsibility for the attack and has threatened to release the PII to the public.[4]

7. On or around July 26, 2024, Defendant began notifying Plaintiffs and Class Members of the Data Breach.

8. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant admits that the unencrypted PII that was accessed and/or acquired by an unauthorized actor.

9. The exposed PII of Plaintiffs and Class Members can be sold on the dark web. Hackers can access and then offer for sale the un-encrypted, unredacted PII to criminals. Plaintiffs and Class Members now face a lifetime risk of (i) identity theft, which is heightened here by the

[3] https://pecofoods.com/our-history/ (last viewed July 29, 2024).
[4] https://www.comparitech.com/news/poultry-processor-peco-foods-notifies-48k-people-of-data-breach-offers-free-credit-monitoring/ (last viewed July 29, 2024).

loss of Social Security numbers, and (ii) the sharing and detrimental use of their sensitive information.

10. The PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiffs and Class Members. Defendant has also purposefully maintained secret the specific vulnerabilities and root causes of the breach and has not informed Plaintiffs and Class Members of that information.

11. Prior to receiving notification, Plaintiffs and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm, including the sharing and detrimental use of their sensitive information. The risk will remain for their respective lifetimes.

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

13. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the disclosure of their private information, and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and

abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

14. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, 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, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiffs and Class Members were compromised through disclosure to an unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

15. On behalf of themselves and the Class as defined herein, Plaintiffs bring claims for negligence, breach of fiduciary duty, breach of confidence, breach of express contract, breach of implied contract, and, in the alternative to their contract-based claims, unjust enrichment. The remedies Plaintiffs seek include actual, nominal, and putative damages; appropriate injunctive and declaratory relief; and attorneys' fees, costs, and expenses.

II. PARTIES

16. Plaintiff Michael Harrison is now and has at all relevant times been a resident and citizen of Missouri, currently residing in Doniphan, Missouri. Plaintiff Harrison was an employee notified of the Data Breach.

17. Plaintiff Allan Carson is now and has at all relevant times been a resident and citizen of Arkansas, currently residing in Pocahontas, Arkansas. Plaintiff Carson was an employee

notified of the Data Breach.

18. Plaintiff Arthur Hughes is now and has at all relevant times been a resident and citizen of Arkansas, currently residing in Jonesboro, Arkansas. Plaintiff Hughes was an employee notified of the Data Breach.

19. Plaintiff Crystal Hargrave is now and has at all relevant times been a resident and citizen of Arkansas, currently residing in Bono, Arkansas. Plaintiff Hargrave was an employee notified of the Data Breach.

20. Plaintiff Kristi Feyjes and has at all relevant times been a resident and citizen of Arkansas, currently residing in Imboden, Arkansas. Plaintiff Feyjes was an employee notified of the Data Breach.

21. Defendant is an Alabama domestic corporation with a principal place of business at 1101 Greensboro Ave., Tuscaloosa, Alabama 35401. Defendant may be served by serving its registered agent, Patrick Noland, at 1101 Greensboro Avenue, Tuscaloosa, Alabama 35401.

22. 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.

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

III. JURISDICTION AND VENUE

24. This Court has subject matter and diversity jurisdiction over this action under 28

U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity.

25. Defendant is a citizen of Alabama because it is a corporation formed under Alabama law with its principal place of business in Tuscaloosa, Alabama.

26. The District of Alabama has personal jurisdiction over Defendant because it conducts substantial business in Alabama and this District and the location of the corporate headquarters that collected and/or stored the PII of Plaintiff and Class Members in this District.

27. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant operates in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District, including Defendant collecting and/or storing the PII of Plaintiffs and Class Members.

IV. FACTUAL ALLEGATIONS

Background

28. Defendant collected the PII of Plaintiffs and Class Members and stored it, unencrypted, on Defendant's internet-accessible network.

29. Plaintiffs and Class Members relied on this sophisticated 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. Plaintiffs and Class Members demand security to safeguard their PII.

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

The Data Breach

31. On or about June 24, 2024, Defendant sent Plaintiffs and Class Members a *Notice of Data Breach* informing Plaintiffs and other Class Members that:

> Peco Foods, Inc. writes to notify you of an incident that may have involved some of your personal information as described below…
>
> **What Happened**
> We recently experienced a network disruption that affected our ability to access certain systems. In response, we promptly initiated an investigation, engaging third-party specialists to assist with understanding the nature and scope of the disruption. As part of our investigation, we have learned that certain information within our systems was subject to unauthorized access on or around December 4, 2023. Upon discovery, we began a thorough review of the data potentially impacted to determine the types of information that may have been impacted and the individuals to whom it relates. On May 23, 2024, this process was completed, and we worked to confirm up-to-date contact information to provide you with notification as soon as possible.
>
> **…**
>
> **What We Are Doing**
> We have taken the steps necessary to address the incident and are committed to fully protecting the information that you have entrusted to us. Upon learning of this incident, we took steps to secure our systems and to enhance the security of our network to prevent similar incidents from occurring in the future. As an additional safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring and identity protection services for a period of <<12/24>> months.[5]

32. Defendant admitted in the *Notice of Data Breach* that an unauthorized actor accessed sensitive information about Plaintiffs and Class Members.

33. The details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

34. The unencrypted PII of Plaintiffs and Class Members may end up for sale on the

[5] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/510ba089-49ff-40d6-b929-1a25878bcd47.html (last viewed July 29, 2024).

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.

35. Defendant 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.

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

37. 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.

38. In 2023, there were at least 22 attacks on companies in the U.S. food and beverage industry, affecting 1,492,481 records. The attack on Peco appears to be the third-largest based on the number of records affected.[6]

39. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[7]

40. The type and breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's customers especially

[6] https://www.comparitech.com/news/poultry-processor-peco-foods-notifies-48k-people-of-data-breach-offers-free-credit-monitoring/

[7] Facts + Statistics: Identity Theft and Cybercrime, INSURANCE INFORMATION INSTITUTE, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-andcybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Apr. 27, 2023).

vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

41. Private Information is a valuable property right.[8] The value of Private Information as a commodity is measurable.[9] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[10] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[11] It is so valuable to identity thieves that once Private Information has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for years afterwards.

42. As a result of their real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, Private Information, and other sensitive information directly on various internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated, and becomes more valuable to thieves and more damaging to victims.

43. 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***

---

[8] See Marc Van Lieshout, The Value of Personal Data, 457 IFIP ADVANCES IN INFORMATION & COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . . . ").

[9] Robert Lowes, Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192.

[10] Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value, OECD (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-andtechnology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[11] U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

in their pursuit of big companies. They breach networks, use specialized tools to maximize 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."[12]

44. 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."[13]

45. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n 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 has been sold or posted on the [Dark] 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."

46. 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. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims' identities to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person,

---

[12] 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 Feb. 24, 2023).

[13] U.S. CISA, Ransomware Guide–September 2020, available at https://www.cisa.gov/stopransomware/ransomware-guide (last visited April 21, 2023).

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.

47. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to exhaust financial accounts, receive medical treatment, open new utility accounts, and incur charges and credit in a person's name.

48. 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 (and 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 freezes on their credit, and correcting their credit reports.

49. 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. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID,

and/or use the victim's information in the event of arrest or court action.

50. Identity thieves can also 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, and/or rent a house or receive medical services in the victim's name.

51. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

52. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[14]

53. 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 big companies such as Defendant, (iii) cybercriminals were leaking corporate information on dark web portals, and (iv) cybercriminals' tactics included threatening to release stolen data.

[14] Janice Y. Tsai et al., The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), https://www.guanotronic.com/~serge/papers/isr10.pdf.

54. In light of the information readily available and accessible on the internet before the Data Breach, 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.

55. 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.

56. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted 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.

Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members.

57. Defendant acquired, collected, and stored the PII of Plaintiffs and Class Members.

58. 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.

59. 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.

60. 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."[15]

[15] See How to Protect Your Networks from RANSOMWARE, at 3, available at

61. 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:

a. 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.

b. 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.

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

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

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

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

g. 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.

h. Configure access controls—including file, directory, and network share

---

https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for- cisos.pdf/view (last visited Feb. 24, 2023).

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.

i. 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.

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

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

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

m. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[16]

62. 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 privileged credentials;

Thoroughly investigate and remediate alerts

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

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

Include IT Pros in security discussions

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

Build credential hygiene

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

Apply principle of least-privilege

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

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[17]

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

64. 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

[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 Feb. 24, 2023).

Data Breach and the exposure of the PII of thousands of individuals, including Plaintiffs and Class Members.

Securing PII and Preventing Breaches

65. 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.

66. 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.

67. 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.

68. The Federal Trade Commission ("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]

[18] 17 C.F.R. § 248.201 (2013).
[19] *Id*.

69. 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.

Value of Personal Identifiable Information

70. 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]

71. 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.

72. 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

[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 visited Feb. 24, 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 visited Feb. 24, 2023).
[22] *In the Dark*, VPN Overview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Feb. 24, 2023.

black market."[23]

73. 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.

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

75. 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.[24]

76. 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 Plaintiff and Class Members as a result of a breach.

77. 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.

---

[23] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit CardNumbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Feb. 24, 2023).

[24] Report to Congressional Requesters, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited Feb. 24, 2023).

78. Defendant was, or should have been, fully aware of the unique type and the significant volume of data contained in Defendant's contract search tool, amounting to potentially tens of thousands of individuals detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

79. To date, Defendant has offered Plaintiffs and Class Members 12 months of complimentary credit monitoring and identify protection services through Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score 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.

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

Plaintiffs' Experiences

81. Plaintiffs were all employees of Defendant before the Data Breach. They received notice from Defendant that their personal information kept by Defendant, their employer, had been compromised as a result of the Data Breach.

82. As a result of the Data Breach, Plaintiffs' sensitive information was accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiffs' sensitive information has been irreparably harmed. For the rest of their lives, Plaintiffs will have to worry about when and how their sensitive information may be shared or used to their detriment.

83. As a result of the Data Breach notice, Plaintiffs spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice of Data Breach* and self-monitoring their accounts. This time has been lost forever and cannot be

recaptured.

84. Additionally, Plaintiffs are very careful about sharing their sensitive PII. They have never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

85. Plaintiffs store any documents containing their sensitive PII in a safe and secure location or destroys the documents. Moreover, they diligently chooses unique usernames and passwords for their various online accounts.

86. Defendant's data security shortcomings resulted in the Data Breach and caused Plaintiffs significant injuries and harm in several ways. For example, Plaintiffs have devoted and will continue to devote significant time, energy, and money to: closely monitoring their bills, records, and credit and financial accounts; changing login and password information on any sensitive account; carefully screening and scrutinizing phone calls, emails, and other communications to ensure that they are not being targeted by identity theft scams, medical identity theft scams, or other attempts at fraud; searching for suitable identity theft protection and credit monitoring services and paying for such services to protect themselves; and placing fraud alerts and/or credit freezes on their credit file. Plaintiffs have taken or will be forced to take these measures to mitigate their potential damages because of the Data Breach.

87. Plaintiffs have suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their PII, especially their Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

88. Plaintiffs have a continuing interest in ensuring that their PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded

from future breaches.

V. CLASS ACTION ALLEGATIONS

89. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure and Local Rule 23.1.

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

> All persons in the United States and its territories whose PII was compromised in the Data Breach, including all individuals who received a data breach notification letter from Defendant. (the "Nationwide Class").

91. Excluded from the Classes 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.

92. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

93. Numerosity, Fed R. Civ. P. 23(a)(1): The Classes are so numerous that joinder of all members is impracticable. Defendant reported that 48,170 were impacted in the Data Breach, and the Classes are apparently identifiable within Defendant's records.[25]

94. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class

[25] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/510ba089-49ff-40d6-b929-1a25878bcd47.html (last viewed July 29, 2024).

Members. These include *inter alia*:

a. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class Members' Private Information from unauthorized access and disclosure;

b. Whether Defendant's actions and its allegedly lax data security practices used to protect Plaintiffs' and Class Members' PII violated the FTC Act and/or other state laws and/or Defendant's other duties alleged herein;

c. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and Class Members;

d. Whether Plaintiffs and Class Members suffered injury as a proximate result of Defendant's negligent actions or failures to act;

e. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class Members' PII;

f. Whether an implied contract existed between Class Members and Defendant providing that Defendant would implement and maintain reasonable security measures to protect and secure Class Members' PII from unauthorized access and disclosure;

g. Whether an express contract existed between class members and Defendant providing that Defendant would implement and maintain reasonable security measures to protect and secure Class Members' PII from unauthorized access and disclosure;

h. Whether Plaintiffs and Class Members are intended third party beneficiaries

of contracts between Defendant and third parties, and if so whether Defendant breached those contracts;

i. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiffs and Class Members;

j. Whether Defendant's actions and inactions alleged herein constitute gross negligence;

k. Whether Defendant breached its duties to protect Plaintiffs and Class Members' Private Information; and

l. Whether Plaintiffs and all other members of the Class are entitled to damages and the measure of such damages and relief.

95. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs on behalf of themselves and all other Class Members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

96. Typicality, Fed. R. Civ. P. 23(a)(3): 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.

97. Policies Generally Applicable to the Classes: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Classes, 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 Classes 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 Classes as a whole, not on facts or law applicable only to Plaintiffs.

98. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Classes. Plaintiffs received the notification of the data breach and have experienced actual damages as a result of the breach. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Classes and the infringement of the rights and the damages they have 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.

99. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): 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.

100. 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 Classes 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.

101. 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 demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

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

103. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to class members' names and addresses affected by the Data Breach. Indeed, class members have already been preliminarily identified and sent notice of the Data Breach.

104. 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.

105. 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(b)(2) of the Federal Rules of Civil

Procedure.

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

a. Whether Defendant 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, and safeguarding 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 an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

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

g. 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;

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

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

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

107. Plaintiffs and the Classes reallege and incorporate by reference herein all the preceding allegations above as if fully alleged herein.

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

109. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiffs and the Classes involved an unreasonable risk of harm to Plaintiffs and the Classes, even if the harm occurred through the criminal acts of a third party.

110. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiffs and the Classes in Defendant's possession was adequately secured and protected.

111. Defendant also had a duty to exercise appropriate clearinghouse practices to remove from an Internet-accessible environment the PII it was no longer required to retain pursuant to regulations and had no reasonable need to maintain in an Internet-accessible environment.

112. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiffs and the Classes.

113. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and the Classes. That special relationship arose because Defendant acquired Plaintiffs and the Classes' confidential PII in the

course of its business practices.

114. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Classes.

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

116. Plaintiffs and the Classes were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Classes, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

117. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Classes. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiffs and the Classes, including basic encryption techniques freely available to Defendant.

118. Plaintiffs and the Classes had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

119. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Classes as a result of the Data Breach.

120. Defendant had and continue to have a duty to adequately disclose that the PII of Plaintiffs and the Classes within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice

was necessary to allow Plaintiffs and the Classes to (i) take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties and (ii) prepare for the sharing and detrimental use of their sensitive information.

121. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and the Classes.

122. Defendant has admitted that the PII of Plaintiffs and the Classes were wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

123. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Classes by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and the Classes during the time the PII was within Defendant's possession or control.

124. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and the Classes in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

125. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiffs and the Classes in the face of increased risk of theft.

126. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Classes by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

127. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove from the Internet-accessible environment any PII it was no longer required to retain pursuant to regulations and which Defendant had no reasonable need to maintain in an Internet-accessible environment.

128. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and the Classes the existence and scope of the Data Breach.

129. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Classes, the PII of Plaintiffs and the Classes would not have been compromised.

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

131. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Classes have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiffs and the Classes; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach

for the remainder of the lives of Plaintiffs and the Classes.

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

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

134. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Classes are entitled to recover actual, consequential, and nominal damage.

COUNT II
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiffs and the Classes)

135. Plaintiffs and the Classes reallege and incorporate by reference herein all the preceding allegations above as if fully alleged herein.

136. Plaintiffs bring this claim individually and on behalf of the Classes.

137. Plaintiffs and Class Members have an interest, both equitable and legal, in their PII that was conveyed to, collected by, and maintained by Defendant and that was accessed or compromised in the Data Breach.

138. As a recipient of customers' PII, Defendant has a fiduciary relationship to its customers, including Plaintiffs and the Class Members.

139. Because of that fiduciary relationship, Defendant was provided with and stored

private and valuable PII related to Plaintiffs and the Classes. Plaintiffs and Class Members were entitled to expect their information would remain confidential while in Defendant's possession.

140. Defendant owed a fiduciary duty under common law to Plaintiffs and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

141. As a result of the parties' fiduciary relationship, Defendant had an obligation to maintain the confidentiality of the information within Plaintiffs' and Class Members' financial records.

142. As a result of the parties' relationship, Defendant had possession and knowledge of confidential PII of Plaintiffs and Class Members, information not generally known.

143. Plaintiffs and Class Members did not consent to nor authorize Defendant to release or disclose their PII to unknown criminal actors.

144. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by, among other things:

a. mismanaging its systems and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII;

b. mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks;

c. failing to design and implement information safeguards to control these risks;

d. failing to adequately test and monitor the effectiveness of the safeguards'

key controls, systems, and procedures;

e. failing to evaluate and adjust its information security program in light of the circumstances alleged herein;

f. failing to detect the breach at the time it began or within a reasonable time thereafter;

g. failing to follow its own privacy policies and practices published to its patients; and

h. failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive PII.

145. But for Defendant's wrongful breach of its fiduciary duties owed to Plaintiffs and Class Members, their PII would not have been compromised.

146. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their PII; Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

b. Costs associated with purchasing credit monitoring and identity theft protection services; Lowered credit scores resulting from credit inquiries following fraudulent activities;

c. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on

compromised accounts;

d. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

e. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

f. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data;

g. and Emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

147. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT III
BREACH OF CONFIDENCE
(On behalf of Plaintiffs and the Classes)

148. Plaintiffs and the Classes reallege and incorporate by reference herein all the preceding allegations above as if fully alleged herein.

149. Plaintiffs bring this claim individually and on behalf of the Classes.

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

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

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

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

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

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

COUNT IV
INVASION OF PRIVACY
(On behalf of Plaintiffs and the Classes)

156. Plaintiffs and the Classes reallege and incorporate by reference herein all the preceding allegations above as if fully alleged herein.

157. Plaintiffs bring this claim individually and on behalf of the Classes.

158. Plaintiffs and Class Members had a reasonable expectation of privacy in the PII Defendant mishandled.

159. Defendant's conduct as alleged above intruded upon Plaintiffs' and Class Members' seclusion under common law.

160. By intentionally failing to keep Plaintiffs' and Class Members' PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiffs' and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiffs' and Class Members' private affairs in a manner that identifies Plaintiffs and Class Members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiffs and Class Members, which is highly offensive and objectionable to an ordinary person; and,

c. Intentionally causing anguish or suffering to Plaintiffs and Class Members.

161. Defendant knew that an ordinary person in Plaintiffs' or Class Members' position would consider Defendant's intentional actions highly offensive and objectionable.

162. Defendant invaded Plaintiffs' and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' private affairs by intentionally misusing and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

163. Defendant intentionally concealed from and delayed reporting to Plaintiffs and Class Members a security incident that misused and/or disclosed their PII without their informed, voluntary, affirmative, and clear consent.

164. The conduct described above was at or directed at Plaintiffs and Class Members.

165. As a proximate result of such intentional misuse and disclosures, Plaintiffs' and Class Members' reasonable expectations of privacy in their PII was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiffs' and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

166. In failing to protect Plaintiffs' and Class Members' PII, and in intentionally misusing and/or disclosing their PII, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private. Plaintiffs, therefore, seeks an award of damages on behalf of themselves and the Classes.

167. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT V
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Classes)

168. Plaintiffs and the Classes reallege and incorporate by reference herein all the preceding allegations above as if fully alleged herein. This claim is pled in the alternative to the breach of express contract claim and all the other claims herein.

169. Plaintiffs bring this claim individually and on behalf of the Classes.

170. When Plaintiffs and Class Members provided their PII to Defendant, they entered into implied contracts with Defendant, under which Defendant agreed to take reasonable steps to protect Plaintiffs' and Class Members' PII, comply with it statutory and common law duties to

protect Plaintiffs' and Class Members' PII, and to timely notify them in the event of a data breach.

171. Defendant solicited and invited Plaintiffs and Class Members to provide their PII as part of Defendant's provision of financial services. Plaintiffs and Class Members accepted Defendant's offers and provided their PII to Defendant.

172. When entering into implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with its statutory and common law duties to adequately protect Plaintiffs' and Class Members' PII and to timely notify them in the event of a data breach.

173. Plaintiffs and Class Members paid money to Defendant to receive financial services. Plaintiffs and Class Members reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

174. Plaintiffs and Class Members would not have provided their PII to Defendant had they known that Defendant would not safeguard their PII, as promised, or provide timely notice of a data breach.

175. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Defendant.

176. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to safeguard Plaintiffs' and Class Members' PII and by failing to provide them with timely and accurate notice of the Data Breach.

177. The losses and damages Plaintiffs and Class Members sustained, include, but are not limited to:

a. Theft of their PII;

b. Costs associated with purchasing credit monitoring and identity theft

protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who

likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

178. As a direct and proximate result of Defendant's breach of contract, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

COUNT VI
BREACH OF EXPRESS CONTRACT
(On behalf of Plaintiffs and the Classes)

179. Plaintiffs and the Classes reallege and incorporate by reference herein all the preceding allegations above as if fully alleged herein. This claim is pleaded in the alternative to the breach of implied contract claim and all the other claims herein.

180. Plaintiffs bring this claim individually and on behalf of the Classes.

181. Defendant's privacy policy created an express contractual obligation to safeguard and protect the sensitive information of Plaintiffs and Class Members.

182. Defendant breached this contractual duty by failing to adequately safeguard Plaintiffs' and Class Members' PII, and by allowing it to be disseminated to unauthorized third parties.

183. Plaintiffs and Class Members substantially performed their part of the bargain.

184. Defendant's breach of this contractual obligation in the privacy policy and elsewhere caused damages to Plaintiffs and Class Members, as set forth herein.

COUNT VII
UNJUST ENRICHMENT
(On behalf of Plaintiff sand the Classes)

185. Plaintiffs and the Classes reallege and incorporate by reference herein all the preceding allegations above as if fully alleged herein.

186. Plaintiffs bring this claim individually and on behalf of the Classes in the alternative to Plaintiffs' contractual based claims pursuant to Fed. R. Civ. P. 8.

187. Plaintiffs and Class Members conferred a monetary benefit on Defendant by providing Defendant with their valuable PII.

188. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead elected to increase its own profits 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 decision to prioritize its own profits over the requisite security.

189. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by its common law and statutory duties.

190. Defendant failed to secure Plaintiffs and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

191. Defendant acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

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

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

194. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class

Members have suffered and will continue to suffer other forms of injury and/or harm.

195. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that it unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

PRAYER FOR RELIEF

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

A. For an Order certifying the Nationwide Class and appointing Plaintiffs and their Counsel to represent such Classes;

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

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

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

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

iii. requiring Defendant to delete, destroy, and purge the personal

identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

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

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

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

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

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

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

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

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

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

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

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

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

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Classes, and to report any deficiencies with compliance of the Court's final judgment;

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

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

F. For prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Dated: July 30, 2024

Respectfully submitted,

/s/ Jason P. Tortorici
Jason P. Tortorici
SBN:
SCHELLECI & TORTORICI, P.C.
100 Centerview Dr., Ste. 205
Birmingham, Alabama 35233
Telephone: (205) 978-4211
jpt@schillecitortoricilaw.com

Leigh S. Montgomery
(*pro hac vice* forthcoming)
Texas Bar No. 24052214
EKSM, LLP
1105 Milford Street

Houston, Texas 77006
Phone: (888) 350-3931
Fax: (888) 276-3455
leigh@ellzeylaw.com

Counsel for Plaintiffs and the Proposed Class