

Wyatt B. Johnson, ISB: 5858
JOHNSON MAY
199 N. Capitol, Suite 200
Boise, Idaho 83702
Telephone: (208) 384-8588
Facsimile: (208) 629-2157
wbj@johnsonmaylaw.com

Attorneys for Plaintiffs

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF IDAHO**

Jason Dallimore, on behalf of himself and all
others similarly situated,

Case No.: _____

Plaintiff,

CLASS ACTION COMPLAINT

v.

DEMAND FOR A JURY TRIAL

Idaho National Laboratory operated by
Battelle Energy Alliance, LLC,

Defendants.

CLASS ACTION COMPLAINT

Plaintiff Jason Dallimore (“Plaintiff”) brings this Class Action Complaint against Idaho National Laboratory (“Defendant”), on behalf of himself and all others similarly situated (“Class Members”), and alleges, upon personal knowledge and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information (“PII”) including, but not limited to names, social security numbers, financial account number, salary information, personal email address, and

home addresses.

2. According to Defendant's website, it is home to over 6,100 researchers and support staff focused on nuclear research.¹

3. To provide these services, and in the ordinary course of Defendant's business, it acquires, possesses, analyzes, and otherwise utilizes the PII of its employees.

4. Defendant is a sophisticated corporation and regularly maintains PII which they know to be sensitive in the ordinary course of business. Defendant is aware of the consequences that would result to employees if the information they maintain were to be compromised and their corresponding obligation to protect against such compromise.

5. Defendant obtained the PII of Plaintiff and Class Members, its employees and their dependents in the ordinary course of business.

6. On or about December 12, 2023, Defendant notified Class Members about the widespread Data Breach (the "Notice Letter"). Upon information and belief, Defendant was targeted in the cyberattack due to the high volume of sensitive PII that it collected and maintained on its computer networks and/or systems and the high value of that information to cyber criminals in facilitating identity theft and fraud.

7. Despite the breach occurring on November 19, 2023, Defendant did not begin informing victims of the Data Breach until December 12, 2023.

8. Indeed, Plaintiff and Class Members were wholly unaware of the Data Breach until they received Notice Letters from Defendant. During this time, Plaintiff and Class Members were unaware that their sensitive PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm.

¹ <https://inl.gov/about-inl/> (last visited December 28, 2023).

9. The Notice Letter provides no further information regarding the Data Breach and only recommends how victims can place a fraud alert or credit freeze on their account and how to sign up for the limited identity monitoring services Defendant offered in response to the Data Breach. The Notice Letter does not explain how the Data Breach occurred, what steps Defendant took following the Data Breach, whether Defendant made any changes to its data security, or most importantly, whether Plaintiff's and Class Members' PII remains in the possession of criminals.

10. By acquiring, utilizing, and benefiting from Plaintiff's and Class Members' PII for its business purposes, Defendants owed or otherwise assumed common law, contractual, and statutory duties that extended to Plaintiff and Class Members. These duties required Defendant to design and implement adequate data security systems to protect Plaintiff's and Class Members' PII in its possession and to keep Plaintiff's and Class Members' PII confidential, safe, secure, and protected from unauthorized disclosure, access, dissemination, or theft.

11. Defendant breached these duties by failing to implement adequate data security measures and protocols to properly safeguard and protect Plaintiff's and Class Members' PII from a foreseeable cyberattack on its systems that resulted in the unauthorized access and theft of Plaintiff's and Class Members' PII.

12. Defendant disregarded the rights of Plaintiff 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 Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the Plaintiff's and Class Members' PII was compromised through disclosure to an unknown and unauthorized criminal third party.

13. Based on the type of sophisticated and targeted criminal activity, the type of PII involved, and Defendant's admission that the PII was accessed, it can be concluded that the unauthorized criminal third party was able to successfully target Plaintiff's and Class Members' PII, infiltrate and gain access to Defendant's network, and exfiltrate Plaintiff's and Class Members' PII, including unencrypted names, dates of birth, and Social Security Numbers, for the purposes of utilizing or selling the PII for use in future fraud and identity theft related cases.

14. As a result of Defendant's failures and the Data Breach, Plaintiff's and Class Members' identities are now at a current and substantial imminent and ongoing risk of identity theft and shall remain at risk for the rest of their lives.

15. Plaintiff 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; (v) failure to receive the benefit of their bargains with Defendant; (vi) nominal damages; (vii) the continued and certainly increased risk to their PII, and damages in an amount equal to the cost of securing identity theft products to assisting in monitoring and protecting them from identity theft, 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 fail to undertake appropriate and adequate measures to protect the PII.

16. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable

measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party.

17. Plaintiff brings this action on behalf of all persons whose PII was compromised due to Defendant's failure to adequately protect Plaintiff's and Class Members' PII. Accordingly, Plaintiff brings this action against Defendants seeking redress for their unlawful conduct and asserts claims on behalf of the Class for Negligence, Breach of Implied Contract, and Unjust Enrichment.

JURISDICTION AND VENUE

18. 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, including Plaintiff, is a citizen of a state different from Defendant to establish minimal diversity.

19. Defendant is a citizen of Idaho because its principal place of business is in Idaho Falls, Idaho and one or more of its members reside in Idaho. Thus, the Federal District of Idaho has general jurisdiction over Defendant.

20. The Federal District of Idaho has personal jurisdiction over Defendant because it conducts substantial business in Idaho and this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

21. 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 Plaintiff's claims occurred in this District.

PARTIES

22. Plaintiff Jason Dallimore is an individual, and has been, at all relevant times, a resident and citizen of Rigby, Idaho.

23. Defendant Idaho National Laboratory is an assumed business name with its principal place of business located at 1955 N. Fremont Ave Idaho Falls, ID 83415. Defendant is headquartered in Idaho.

FACTUAL ALLEGATIONS

Background

24. Plaintiff and Class Members, who are past and current employees or dependents of Defendant, provided and entrusted Defendant and the others with sensitive and confidential information, including but not limited to their names, dates of birth, and Social Security numbers.

25. Defendant is a national laboratory focused on nuclear research, renewable energy systems, and security solutions.

26. As a condition of being a past or current employee or dependent of an employee of Defendant, Defendant required that Plaintiff and Class Members entrust it with highly confidential PII.

27. Plaintiff and Class Members relied on the 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. Plaintiff and Class Members value the integrity and confidentiality of their PII and demand security to safeguard their PII.

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

29. In addition to Plaintiff and Class Members' complete dependence on Defendant to protect their PII, because this was a readily foreseeable and preventable data breach, and Defendant represented that they valued and would protect the PII of Plaintiff and Class Members, Defendant had duties to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties.

The Data Breach

30. On or about December 12, 2023, Defendant began sending Plaintiff and other Data Breach victims a Notice of Data Incident letter (the "Notice Letter"), informing them that:

What Happened? On November 20, 2023, INL was informed that a cyber data breach occurred on November 19, 2023, at an off-site data center that housed information on INL employees, former employees, spouses, and dependents. The event did not impact INL's own network or other networks or databases used by employees, lab customers or other contractors. The event continues to be investigated by federal agencies including the Department of Energy, Federal Bureau of Investigation, and the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency. Though the matter is currently under investigation, this notice was not delayed as a result of law enforcement investigations.

What Information Was Involved? We can confirm that multiple forms of sensitive personally identifiable information (PII) including names, social security numbers, salary information and banking details were exposed for many individuals. Some individuals only had their names and dates of birth compromised.

The compromised information contained payroll data for employees, former employees, and retirees that was current as of June 1, 2023. PII that may have been included within that data set includes the following: full name, date of birth, social security number, financial account number, salary information, personal email address, and/or home address.²

31. On or about November 20, 2023, Defendant notified various state Attorneys General of the Data Breach, including the Attorneys General of Maine, and provided them “sample” notices of the Data Breach. In total, at least 45,047 individuals’ data was compromised by the Data Breach.³

32. Defendant admitted in the Notice Letter that an unauthorized actor accessed and obtained sensitive information about Plaintiff and Class Members, including their names, dates of birth, and Social Security Numbers. Upon information and belief, this PII was accessible, unencrypted, unprotected, and vulnerable to acquisition and/or exfiltration by the unauthorized actor.

33. In response to the Data Breach, Defendant claims that it has “[restricted] access to the server that was involved in the breach, alerted federal law enforcement agencies, and began the process of confirming the individuals and the types of information that were compromised...”⁴ However, 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

² The Notice of Data Incident/Breach Letter (the “Notice Letter”.) A sample copy is available at <https://apps.web.maine.gov/online/aeviewer/ME/40/ff925db5-9987-4a47-a5bc-a89c94f794f5.shtml> (last visited Dec. 28, 2023).

³See *Data Breach Notifications*, Office of the Maine Attorney General, <https://apps.web.maine.gov/online/aeviewer/ME/40/ff925db5-9987-4a47-a5bc-a89c94f794f5.shtml> (last visited Dec. 28, 2023).

⁴See Notice Letter.

regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

34. As a result of the Data Breach, the unencrypted PII of Plaintiff and Class Members will end up for sale on the dark web or fall into the hands of companies that will use the detailed PII for targeted marketing without the consent of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

35. While Defendant stated in the Notice Letter that the unusual activity occurred on November 19, 2023 and was discovered on November 20, 2023. Defendant did not begin notifying victims until December 12, 2023.⁵

36. Defendant waited over 30 days to disclose the Data Breach to Plaintiff and Class Members. During this time Plaintiff and Class Members had no idea their PII had been compromised in the Data Breach, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

37. Defendant has offered abbreviated, non-automatic credit monitoring services to victims thereby identifying the harm posed to Plaintiff and Class Members as a result of the Data Breach, which does not adequately address the lifelong harm that victims face following the Data Breach. Indeed, the Data Breach involves PII that cannot be changed, such as Social Security numbers.

The Data Breach Was Foreseeable

38. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in many industries preceding the date of

⁵ *Id.*

the breach.

39. Because Defendant had duties to protect Plaintiff's 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.

40. In the years immediately preceding the Data Breach, Defendant knew or should have known that its computer systems were a target for cybersecurity attacks, including attacks involving data theft, because warnings were readily available and accessible via the internet. In addition to articles in the public press about the extensive number of data breaches affecting companies throughout all industries, governmental agencies have constantly sent and published notices of the need for companies who maintain sensitive personal information to carefully safeguard the sensitive and valuable information collected from consumers.

41. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.⁶

42. Indeed, cyberattacks on business analytics companies like Defendant have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, potential attack.⁷

43. This readily available and accessible information confirms that, prior to the Data Breach, Defendants knew or should have known that (i) unauthorized actors were targeting companies such as Defendant, (ii) unauthorized actors were aggressive in their pursuit of

⁶ See 2021 Data Breach Annual Report, ITRC 6 (Jan. 2022), available at <https://www.idtheftcenter.org/notified> (last visited Dec. 3, 2023).

⁷ *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware> (last visited Dec. 3, 2023).

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

44. Given Defendant's knowledge that the sensitive information it maintained would be targeted by hackers, Defendant had a duty to institute appropriate data security procedures to guard against this threat.

45. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store that PII in an Internet-accessible environment, had reason to be on guard for the targeting and exfiltration of the PII at issue here. Defendant had cause to be particularly on guard against such an attack as a result of their foreknowledge as demonstrated in their public representations.

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

47. Prior to the Data Breach, Defendant knew or should have known that they 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 Had an Obligation to Protect the PII

48. Defendant's failure to adequately secure Plaintiff's and Class Members' PII breaches duties it owes Plaintiff and Class Members under statutory and common law. Moreover, Plaintiff and Class Members surrendered their highly sensitive personal data to Defendant under the implied condition that Defendants would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their data, independent of any statute.

49. Defendant was prohibited by the Federal Trade Commission Act (the "FTC Act")

(15 U.S.C. § 45) from engaging in “unfair or deceptive acts or practices in or affecting commerce.” The Federal Trade Commission (the “FTC”) has concluded that a company’s failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information is an “unfair practice” in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

50. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendant’s possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII of Plaintiff and Class Members.

51. Defendant owed a duty to Plaintiff and Class Members to design, maintain, and test its computer systems, servers, and networks to ensure that the PII in its possession was adequately secured and protected.

52. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including not sharing information with other entities who maintained substandard data security systems.

53. Defendant owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach on its data security systems in a timely manner.

54. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

55. Defendant owed a duty to Plaintiff and Class Members to disclose if its computer

systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust this PII to Defendant.

56. Defendant owed a duty of care to Plaintiff and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

57. Defendant owed a duty to Plaintiff and Class Members to encrypt and/or more reliably encrypt Plaintiff's and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

58. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and 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.

59. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to, at least, tens of thousands of individuals' PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

Value of PII

60. The PII of individuals remains of high value to criminals, as evidenced by the prices criminals 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 \$200.⁸ Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.⁹ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹⁰

61. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly \$200 billion.¹¹

62. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.¹²

63. Conversely sensitive PII can sell for as much as \$363 per record on the dark web according to the Infosec Institute.¹³

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

⁸ Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends (Oct. 16, 2019), <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Dec. 3, 2023).

⁹ Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Dec. 3, 2023).

¹⁰ *In the Dark*, VPNOOverview, 2019, *available at*: <https://vpnooverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Dec. 3, 2023).

¹¹ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers> (last visited Dec. 3, 2023).

¹² Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, *available at* <https://computermobilepanel.nielsen.com/ui/US/en/faen.html> (last visited Dec. 3, 2023).

¹³ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last visited Dec. 3, 2023).

additional loss of value.

65. 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.^{14, 15}

66. Based on the foregoing, the information compromised in the Data Breach, including full names matched with Social Security numbers, 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.

67. 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.”¹⁶

68. 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.

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

¹⁴ <https://datacoup.com> (last visited Dec. 3, 2023).

¹⁵ <https://digi.me/what-is-digime/> (last visited Dec. 3, 2023).

¹⁶ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Dec. 3, 2023).

[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 has 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.¹⁷

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

71. Plaintiff and Class Members now face a lifetime of constant surveillance of their financial and personal records, credit monitoring, and loss of rights. Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

72. Defendant has acknowledged the risk and harm caused to Plaintiff and Class Members as a result of the Data Breach. Defendant, to date, has offered Plaintiff and Class Members abbreviated, non-automatic credit monitoring services. The limited credit monitoring is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here. Moreover, Defendant put the burden squarely on Plaintiff and Class Members to enroll in the inadequate monitoring services.

Data Breaches Are Preventable

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

74. Defendant did not use reasonable security procedures and practices appropriate to

¹⁷ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last visited Dec. 3, 2023).

the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of PII, such as encrypting the information or deleting it when it is no longer needed.

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

76. 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.”¹⁸

77. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.

¹⁸ 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 Nov. 29, 2023).

- 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.¹⁹

78. To prevent and detect cyber-attacks or ransomware attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

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

¹⁹ *Id.* at 3-4.

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].²⁰

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

80. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of more than fifty thousand individuals, including that of Plaintiff and Class Members.

81. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is

²⁰ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at*: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Nov. 29, 2023).

exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendants Acquire, Collect, And Store Customers' PII

82. Defendant acquire, collect, and store a massive amount of PII on its customers, former customers, and other personnel.

83. As a condition of obtaining employment from Defendant, Defendant required that employees entrust it with highly sensitive personal information.

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

85. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII and would not have entrusted it to Defendant absent a promise to safeguard that information.

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

87. Plaintiff and the Class Members 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.

Defendant Knew or Should Have Known, of the Risk Because Companies in Possession of PII are Particularly Susceptible To Cyber Attacks

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

89. Data breaches, including those perpetrated against financial institutions that store PII in their systems, have become widespread.

90. In the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.²¹

91. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million customers, March 2019), University of Washington Medicine (974,000 customers, December 2018), Florida Orthopedic Institute (640,000 customers, July 2020), Wolverine Solutions Group (600,000 customers, September 2018), Oregon Department of Human Services (645,000 customers, March 2019), Elite Emergency Physicians (550,000 customers, June 2020), Magellan Health (365,000 customers, April 2020), and BJC Health System (286,876 customers, March 2020), Defendants knew or should have known that its electronic records would be targeted by cybercriminals.

92. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store PII are "attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly."²²

93. Additionally, as companies became more dependent on computer systems to run

²¹ See <https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/> (last visited Nov. 29, 2023).

²²https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last visited Nov. 29, 2023).

their business,²³ e.g., working remotely as a result of the Covid-19 pandemic, and the Internet of Things (“IoT”), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.²⁴

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

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

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

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

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

99. As a financial institution in custody of current and former customers’ PII,

²³<https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html> (last visited Nov. 29, 2023).

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

Value of Personally Identifying Information

100. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”²⁵ 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.”²⁶

101. 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.²⁷ For example, Personal Information can be sold at a price ranging from \$40 to \$200.²⁸ Criminals can also purchase access to entire company data breaches from \$900 to

²⁵ 17 C.F.R. § 248.201 (2013).

²⁶ *Id.*

²⁷ *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/>

²⁸ *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/>

\$4,500.29

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

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.³⁰

103. 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.

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

²⁹ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/>

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

inherited into the new Social Security number.”³¹

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

106. 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.”³²

107. 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.

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

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.

³¹ Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last visited Nov. 29, 2023).

³² Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Nov. 29, 2023).

As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.³³

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

Defendant Fails to Comply with FTC Guidelines

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

111. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies to correct any security problems.³⁴

112. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the

³³ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last visited Nov. 29, 2023).

³⁴ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Nov. 29, 2023).

system; and have a response plan ready in the event of a breach.³⁵

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

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

115. These FTC enforcement actions include actions against financial institutions, like Defendant.

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

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

118. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII or to comply with applicable industry standards

³⁵ *Id.*

constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

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

Defendant Fails to Comply with Industry Standards

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

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

122. Other best cybersecurity practices that are standard for financial institutions 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. Defendants

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

123. 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.

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

125. As result of Defendant's ineffective and inadequate data security practices, Plaintiff and Class Members now face a present and ongoing risk of fraud and identity theft.

126. Due to the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) diminution or loss of value of their PII; and (i) the continued risk to their PII, which remains in Defendant's possession, and which is subject to further breaches, so

long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

The Risk of Identity Theft to Plaintiff and Class Members is Present and Ongoing

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

128. 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.

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

130. The Dark Web is an unindexed layer of the internet that requires special software or authentication to access.³⁶ 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

³⁶ Louis DeNicola, *What Is the Dark Web?*, Experian (May 12, 2021), <https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/> (last visited Dec. 3, 2023).

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.³⁷ This prevents Dark Web marketplaces from being easily monitored by authorities or accessed by those not in the know.

131. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the PII at issue here.³⁸ 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 financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.³⁹ As Microsoft warns “[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others.”⁴⁰

132. 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

³⁷ *Id.*

³⁸ *What is the Dark Web?* – Microsoft 365 (July 15, 2022), <https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web> (last visited Dec. 3, 2023).

³⁹ *Id.*; see also Louis DeNicola, *supra* note 25.

⁴⁰ *Id.*

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.⁴¹

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.

133. Even then, a 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.”⁴²

134. 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 being 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 additional credit lines.⁴³

135. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime

⁴¹ Social Security Administration, *Identity Theft and Your Social Security Number* (2021), available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Dec. 3, 2023).

⁴² 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 Dec. 3, 2023).

⁴³ *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2021), <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Dec. 3, 2023).

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.⁴⁴

136. Further, according to the same report, “rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good.”⁴⁵ Defendants did not rapidly report to Plaintiff and Class Members that their PII had been stolen.

137. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

138. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII. 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.

139. 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, Plaintiff and Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

140. The Federal Trade Commission (“FTC”) has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that “most consumers cannot begin to comprehend the types and

⁴⁴ See *2019 Internet Crime Report*, FBI (Feb. 11, 2020), <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120> (last visited Dec. 3, 2023).

⁴⁵ *Id.*

amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit.”⁴⁶

141. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.⁴⁷

142. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers’ finances, credit history and reputation, and can take time, money, and patience to resolve the fallout. The FTC treats 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(a) of the FTC Act.⁴⁸

143. Defendant’s failure to properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff’s and Class Members’ injury by depriving them of the earliest ability

⁴⁶ Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), FTC (Dec. 7, 2009), <http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf> (last visited Dec. 3, 2023).

⁴⁷ See generally <https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business> (last visited Dec. 3, 2023).

⁴⁸ See, e.g., *Protecting Personal Information: A Guide for Business*, FTC, <https://www.ftc.gov/news-events/news/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices> (last visited Dec. 3, 2023).

to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

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

144. 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 or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

145. Thus, due to Defendant’s admitted recognition of the actual and imminent risk of identity theft, Defendant offered Plaintiff and Class Members abbreviated, non-automatic credit monitoring services.

146. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing “freezes” and “alerts” with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

147. Plaintiff’s mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”⁴⁹

⁴⁹ See U.S. GOV’T ACCOUNTABILITY OFF., GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER,

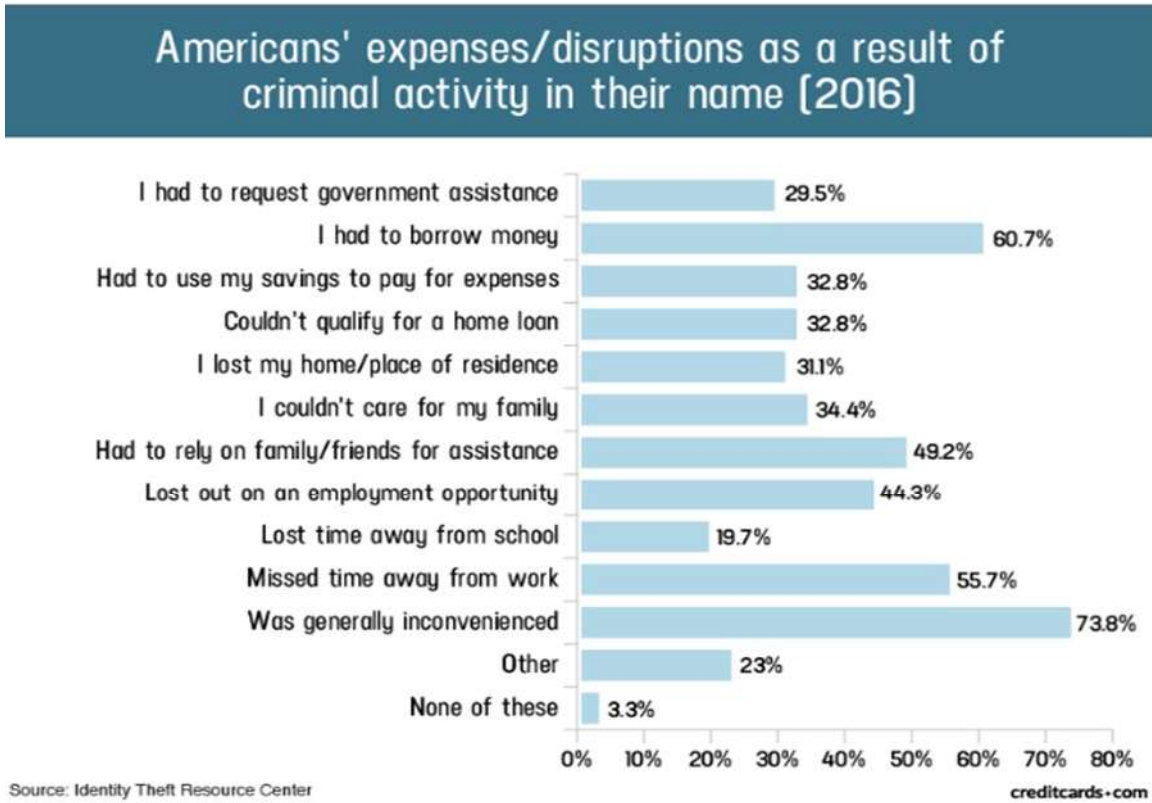
148. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.⁵⁰

149. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:⁵¹

THE FULL EXTENT IS UNKNOWN (2007) ("GAO Report"), available at <https://www.gao.gov/new.items/d07737.pdf> (last visited Dec. 3, 2023).

⁵⁰ See Federal Trade Commission, IdentityTheft.gov, <https://www.identitytheft.gov/Steps> (last visited Dec. 3, 2023).

⁵¹ "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: <https://web.archive.org/web/20190304002224/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php> (last visited Dec. 3, 2023).



150. Indeed, the FTC recommends that identity theft victims take several steps and spend time 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 7 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.⁵²

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

151. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach.

152. The abbreviated, non-automatic credit monitoring offered to persons whose PII was

⁵² See Federal Trade Commission, IdentityTheft.gov, <https://www.identitytheft.gov/Steps> (last visited Dec. 3, 2023).

compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face ongoing identity theft and financial fraud for the remainder of their lives. Defendant also place the burden squarely on Plaintiff and Class Members by requiring them to independently sign up for that service, as opposed to automatically enrolling all victims of this Data Breach.

153. 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; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

154. It must be noted there may be a substantial time lag – measured in years – between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used.

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

156. 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.⁵³ The information disclosed in this Data Breach is impossible to “close” and difficult, if not impossible, to change (such as Social Security numbers).

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

158. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year, or more, 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 minimum of five years that Plaintiff and Class Members would not need to bear but for Defendant’s failure to safeguard their PII.

A. Injunctive Relief Is Necessary to Protect against Future Data Breaches

159. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing PII is not accessible online and that access to such data is password protected.

Plaintiff Jason Dallimore’s Experience

160. At the time of the Data Breach, Defendant retained Plaintiff Dallimore’s PII in its system.

161. Plaintiff Dallimore was sent a Notice Letter on December 12, 2023, informing him

⁵³ 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> (last visited Dec. 4, 2023)

that Defendant had experience a Data Breach and that Plaintiff's PII, including his full name, date of birth, and Social Security Number was compromised in the Breach.

162. As a result of the Data Breach, Plaintiff Dallimore spent time dealing with the consequences of the Data Breach, which includes verifying the legitimacy of the Notice Letter, and self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at Defendant's direction by way of the Notice Letter where Defendant advised Plaintiff Dallimore to mitigate his damages by, among other things, freezing his credit accounts and monitoring his accounts for fraudulent activity.

163. Plaintiff Dallimore is a cautious person and is therefore very careful about sharing sensitive PII. As a result, he has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Dallimore stores any documents containing her PII in a safe and secure location or destroys the documents. Moreover, Plaintiff Dallimore diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be.

164. Plaintiff Dallimore only allowed Defendant to maintain, store, and use his PII because he believed that Defendant would use basic security measures to protect her PII, such as requiring passwords and multi-factor authentication to access databases storing his PII. As a result, Plaintiff's PII was within the possession and control of Defendant at the time of the Data Breach.

165. In the instant that his PII was accessed and obtained by a third party without his consent or authorization, Plaintiff suffered injury from a loss of privacy.

166. Plaintiff Dallimore has been further injured by the damages to and diminution in value of his PII—a form of intangible property that Plaintiff entrusted to Defendant. This

information has inherent value that Plaintiff was deprived of when his PII was placed on a publicly accessible database, exfiltrated by cybercriminals, and, upon information and belief, later placed for sale on the dark web.

167. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendants have still not fully informed him of key details about the Data Breach's occurrence.

168. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

169. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

170. Plaintiff Dallimore is aware of no other source from which the theft of his PII could have come. He regularly takes steps to safeguard his own PII in his own control.

171. Given the time Plaintiff Dallimore has lost investigating this data breach, taking steps to understand its full scope, determining the appropriate remedial steps, contacting counsel, etc., coupled with Plaintiff Dallimore's resultant and naturally foreseeable fears/concerns for the use of Plaintiff Dallimore's valuable PII, the damages articulated more specifically above are far from the full extent of the harm thereto.

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

CLASS ALLEGATIONS

173. Plaintiff brings this nationwide class action on behalf of himself 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.

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

All individuals whose PII was compromised in the data breach that is the subject of the Notice of Security Incident that Idaho National Laboratory sent to Plaintiff and Class Members on or around November 20, 2023 (the “Class”).

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

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

176. Numerosity: The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. According to the breach report submitted to the Office of the Maine Attorney General, at least 45,000 Class Members were impacted in the Data Breach.⁵⁴ The Class is apparently identifiable within Defendants’ records, and Defendants have already identified these individuals (as evidenced by sending them breach notification letters).

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

⁵⁴See <https://apps.web.maine.gov/online/aeviewer/ME/40/ff925db5-9987-4a47-a5bc-a89c94f794f5.shtml> (last visited Dec. 28, 2023).

- a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;
 - b. Whether Defendant had respective duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;
 - c. Whether Defendant had respective duties not to use the PII of Plaintiff and Class Members for non-business purposes;
 - d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;
 - e. Whether and when Defendant actually learned of the Data Breach;
 - f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;
 - g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;
 - h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
 - i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
 - j. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;
 - k. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.
178. Typicality: Plaintiff's claims are typical of those of the other members of the Class

because Plaintiff, like every other Class Member, was exposed to virtually identical conduct and now suffers from the same violations of the law as each other member of the Class.

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

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

181. 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 Defendants. 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.

182. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

183. 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.

184. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

185. 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.

186. Further, Defendant has acted on grounds that apply generally to the Class as a

whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

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

- a. Whether Defendant failed to timely notify the Plaintiff and the class of the Data Breach;
- b. Whether Defendants owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;
- c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;
- d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer PII; and Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT I

Negligence

(On Behalf of Plaintiff and the Class)

188. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

189. Defendant require its employees, including Plaintiff and Class Members, to submit non-public PII in the ordinary course of providing its financial services.

190. Defendant gathered and stored the PII of Plaintiff and Class Members as part of its business of soliciting its services to its customers, which solicitations and services affect commerce.

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

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

193. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

194. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

195. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks adequately protected the PII.

196. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and Class Members. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part of being employees of Defendant.

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

198. Defendant was subject to an "independent duty," untethered to any contract between Defendants and Plaintiff or the Class.

199. Defendants also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII it was no longer required to retain pursuant to regulations.

200. Moreover, Defendant had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach.

201. Defendant had and continue to have a duty to adequately disclose that the PII of Plaintiff and the Class 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 Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

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

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Allowing unauthorized access to Class Members' PII;
- d. Failing to detect in a timely manner that Class Members' PII had been compromised;
- e. Failing to remove former customers' PII it was no longer required to retain pursuant to regulations,
- f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and
- g. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

203. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect 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 the immense damages that would result to Plaintiff and the Class.

204. Plaintiff and Class Members are within the class of persons the Federal Trade Commission Act intended to protect and the type of harm that resulted from the Data Breach was the type of harm these statutes were intended to guard against.

205. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

206. 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 Plaintiff and the Class.

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

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

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

210. Plaintiff and the Class 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 Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems or transmitted through third party systems.

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

212. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

213. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

214. Defendant's duty extended to protecting Plaintiff 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 have also recognized the existence of a specific duty to reasonably safeguard personal information.

215. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

216. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

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

218. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (viii) Plaintiff's PII being disseminated on the dark web, according to Credit Sesame; (ix) statutory damages; (x) nominal damages; and (xi) 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) remains 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.

219. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class 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 Defendants fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

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

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

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

222. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

223. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendants have a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

224. Defendant breached its duties to Plaintiff and Class Members under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to

safeguard Plaintiff's and Class Members' PII.

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

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

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

228. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that they 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 PII.

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

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

230. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

231. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of receiving financial services from Defendant.

232. Plaintiff and the Class entrusted their PII to Defendant. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard

and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

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

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

235. The mutual understanding and intent of Plaintiff and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

236. Defendant solicited, offered, and invited Plaintiff and Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

237. In accepting the PII of Plaintiff and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the PII from unauthorized access or disclosure.

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

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

240. Plaintiff and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

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

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

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

244. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

245. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiff and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

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

247. Plaintiff and Class Members are also entitled to injunctive relief requiring

Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

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

248. Plaintiff re-alleges and incorporates by reference all preceding allegations, as if fully set forth herein.

249. Plaintiff brings this Count in the alternative to the breach of implied contract count above.

250. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided services to Defendant and/or its agents through employment and in so doing also provided Defendant with their PII. In exchange, Plaintiff and Class Members should have received from Defendant the services that were the subject of the transaction and should have had their PII protected with adequate data security.

251. Defendant knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the PII entrusted to it. Defendant profited from Plaintiff's retained data and used Plaintiff's and Class Members' PII for business purposes.

252. Defendant failed to secure Plaintiff's and Class Members' PII and, therefore, did not fully compensate Plaintiff or Class Members for the value that their PII provided.

253. Defendant acquired the PII through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

254. If Plaintiff and Class Members had known that Defendant would not use adequate

data security practices, procedures, and protocols to adequately monitor, supervise, and secure their PII, they would have entrusted their PII at Defendant or obtained services at Defendant.

255. Plaintiff and Class Members have no adequate remedy at law.

256. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

257. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) experiencing an increase in spam calls, texts, and/or emails; (ix) statutory damages; (x) nominal damages; and (xi) 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) remains 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.

258. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.

259. Plaintiff and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the

alternative to, other claims pleaded herein.

PRAYER FOR RELIEF

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

- A. For an Order certifying the Class, and appointing Plaintiff and his Counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
 - i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
 - iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
 - iv. requiring Defendant to provide out-of-pocket expenses associated with the

prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII for Plaintiff's and Class Members' respective lifetimes;

- v. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;
- vi. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;
- vii. 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;
- viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- x. requiring Defendant to segment data by, among other things, creating firewalls and controls so that if one area of Defendant's network is compromised, hackers cannot gain access to portions of Defendant's systems;
- xi. requiring Defendant to conduct regular database scanning and securing

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

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

- D. For an award of damages, including actual, nominal, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMAND

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

Respectfully Submitted,

Date: January __, 2024


/s/_____

Bryan L. Bleichner*
Philip J. Krzeski*
CHESTNUT CAMBRONNE PA
100 Washington Ave., Ste. 1700
Minneapolis, MN 55401
Telephone: (612) 339-7300
Facsimile: (612) 336-2940
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

*Attorneys for Plaintiff Jason Dallimore and the
Putative Class*

** PRO HAC VICE FORTHCOMING*

DATED this 26th day of January, 2024.


Wyatt B. Johnson (Jan 26, 2024 15:55 MST)

Wyatt B. Johnson
Attorneys for Plaintiff

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Nuclear Research Facility Idaho National Laboratory Facing Data Breach Lawsuit Over Nov. 2023 Cyberattack](#)
