UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

IN RE: MOVEIT CUSTOMER DATA SECURITY BREACH LITIGATION This Document Relates To: PATRICIA MARSHALL, *individually and on behalf of all others similarly situated*, Plaintiff, v. TEACHERS INSURANCE AND ANNUITY ASSOCIATION OF AMERICA, PENSION BENEFIT INFORMATION, LLC, and PROGRESS SOFTWARE CORPORATION, Defendants.	MDL NO. 1:23-md-03083-ADB-PGL **AMENDED CLASS ACTION COMPLAINT** CIVIL ACTION NO. 1:23-cv-12787

Plaintiff Patricia Marshall ("Plaintiff"), individually and on behalf of all others similarly situated, hereby brings this Class Action Complaint against Teachers Insurance and Annuity Association of America ("TIAA"), Pension Benefit Information, LLC ("PBI"), and Progress Software Corporation ("PSC") (together with TIAA and PBI, "Defendants") and alleges, upon personal knowledge as to her own actions and her counsel's investigations, and upon information and good faith belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff incorporates the allegations contained in Plaintiffs' Omnibus Set of Additional Pleading Facts (ECF No. 908) in its entirety.

2. Plaintiff brings this class action against Defendants for their abject failure to properly secure and safeguard personally identifiable information ("PII") including Plaintiff's and

Class Members' names, Social Security numbers, gender, dates of birth, and addresses (collectively, "Private Information" or "PII"). Defendants' severe failures have affected—and continue to affect—millions people.[1]

3. On or about May 31, 2023, TIAA was notified that an unauthorized third-party had exploited a vulnerability in the software that Defendants used to transfer files containing sensitive information. A subsequent investigation determined that there was a cybersecurity incident between May 29, 2023 and May 30, 2023 during which unauthorized third parties accessed Plaintiff's and Class Members' Private Information.

4. As explained in detail herein, an unauthorized third party accessed Defendants' MOVEit Transfer servers and accessed and removed PII from the server as early as May 27, 2023[2] (the "Data Breach").

5. The investigation into the Data Breach confirmed that an unauthorized actor accessed certain files containing Plaintiff's and Class Members' Private Information, including names, social security numbers, dates of birth, gender, and addresses.

6. Based on the Notice Letter, Defendants admit that Plaintiff's and Class Members' Private Information was unlawfully accessed by a third party.

7. Upon information and good faith belief, Defendants were on notice of the high potentiality for this exact sort of data security incident and yet maintained the Private Information in a negligent manner. In particular, the Private Information was maintained on computer systems

[1] According to the report submitted to the Office of the Maine Attorney General, 2,372,076 of TIAA's customers were impacted in the Data Breach. See https://apps.web.maine.gov/online/aeviewer/ME/40/ed67df63-aced-4ecb-91ce-602c7e34c83a.shtml (last visited Sept. 11, 2023).

[2] https://www.reuters.com/technology/hackers-use-flaw-popular-file-transfer-tool-steal-data-researchers-say-2023-06-02/; https://news.yahoo.com/another-calpers-retiree-sues-pbi-231108178.html.

and networks that were in a condition vulnerable to cyberattack. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendants and, thus, Defendants were on notice that failing to take appropriate protective measures would expose and increase the risk that the Private Information could be compromised and stolen.

8. Defendants owed a non-delegable duty to Plaintiff and Class Members to implement and maintain reasonable and adequate security measures to secure, protect and safeguard their Private Information against unauthorized access and disclosure including, but not limited to, ensuring that the third parties that they contracted with likewise implemented appropriate data security protection measures.

9. As a result of Defendants' inadequate vendor screening, security measures and breach of their legal duties and obligations, the aforementioned data breach occurred, and Plaintiff's and Class Members' PII was accessed and "stolen" by an unspecified "bad actor." Defendants permitted Plaintiffs' and Class Members' PII to be held in unencrypted form despite the heightened sensitivity of such PII.

10. As a result, Plaintiff's and Class Members' Private Information has been compromised and they now face an ongoing risk of identity theft, which is heightened here by the loss of Social Security numbers – the gold standard for identity thieves. The exposed Private Information of Plaintiff and Class Members can, and likely will, be sold repeatedly on the dark web.

11. In addition to the ongoing risk of identity theft, those impacted by the Data Breach have suffered and will suffer numerous actual and concrete injuries and damages, including: (a) invasion of privacy; (b) financial "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; (d) financial "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 of value of their Private Information; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

12. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, future costs of identity theft monitoring, and injunctive relief including improvements to Defendants' data security systems, and future annual audits.

13. Plaintiff therefore brings this class action lawsuit on behalf of those similarly situated to address Defendants' inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed. Accordingly, Plaintiff brings this action against Defendants seeking redress for their unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence *per se*, (iii) breach of fiduciary duty; (iv) unjust enrichment; (v) violations of the New York Deceptive Trade Practices Act, N.Y. Gen. Bus. Law § 349 *et seq*.; (vi) breach of implied contract; and (vii) declaratory judgment.

PARTIES

14. Plaintiff Patricia Marshall is a citizen of the State of Vermont residing in Chittenden County, Vermont.

15. Plaintiff received a letter dated August 11, 2023 from PBI notifying her that Defendants' network had been accessed and that her Private Information may have been involved in the Data Breach.

16. Defendant, Teachers Insurance and Annuity Association of America, is a New York based stock insurance company with its principal place of business located at 730 Third Avenue, New York, New York 10017.

17. TIAA provides services to over 5 million clients from more than 15,000 institutions and manages nearly $1 trillion in assets with holdings in more than 50 countries.

18. TIAA is a Vendor Contracting Entity of PBI. *See* Plaintiffs' Omnibus Set of Additional Pleading Facts, Appendix A.

19. PBI is a for-profit Delaware corporation with its principal place of business at 333 S 7th Street, Suite 2400, Minneapolis, MN 55402. PBI uses PSC's MOVEit service in the regular course of its business acting as a pension plan "sponsor, administrator, or record keeper" "for thousands of organizations" and pension plans.[3]

20. PBI is a PSC Vendor. *See* Plaintiffs' Omnibus Set of Additional Pleading Facts, Appendix A.

21. PSC is a Delaware corporation and maintains its headquarters and principal place of business at 15 Wayside Road, 4th Floor, Burlington, Massachusetts 01803. PSC offers the service MOVEit, which experienced the Data Breach underlying Plaintiff's claims.

[3] https://www.pbinfo.com/ (last visited August 1, 2023).

JURISDICTION & VENUE

22. This case was originally filed in the Southern District of New York. This action was transferred to this Court for coordinated or consolidated pretrial proceedings pursuant to 28 U.S.C. § 1407 and Rule 7.1 of the Rules of Procedure of the United States Judicial Panel on Multidistrict Litigation.

23. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiff and at least one member of the Class, as defined below, is a citizen of a different state than Defendants, there are more than 100 putative class members, and the amount in controversy exceeds $5 million, exclusive of interest and costs. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

24. The United States District Court for the Southern District of New York has personal jurisdiction over Defendants because TIAA's principal place of business is in that District and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from that District. Defendants have sufficient contacts in New York, as they conduct a significant amount of business in the state of New York.

25. Venue is proper in the United States District Court for the Southern District of New York under 28 U.S.C. § 1391(a) through (d) because a substantial part of the events giving rise to this action occurred in that District, including decisions made by TIAA's governance and management personnel or inaction by those individuals that led to the Data Breach; TIAA's principal place of business is located in that District; TIAA maintains Class Members' PII in that District; and TIAA caused harm to Class Members residing in that District.

FACTUAL ALLEGATIONS

Background

26. TIAA is a financial services and insurance company that services roughly 5 million clients from over 15,000 organizations across the United States.

27. Upon information and belief, in the course of collecting PII from its clients, including Plaintiff, Defendants promised to provide confidentiality and adequate security for client data through their applicable privacy policies and through other disclosures in compliance with statutory privacy requirements.

28. Indeed, TIAA's Privacy Notice provides that: "TIAA protects the personal information you provide against unauthorized access, disclosure, alteration, destruction, loss, or misuse. Your personal information is protected by physical, electronic, and procedural safeguards in accordance with federal and state standards. These safeguards include appropriate procedures for access and use of electronic data, provisions for the secure transmission of sensitive personal information on our website, and telephone system authentication procedures. Additionally, we limit access to your personal information to those TIAA employees and agents who need access in order to offer and provide products or services to you. We also require our service providers to protect your personal information by utilizing the privacy and security safeguards required by law."[4]

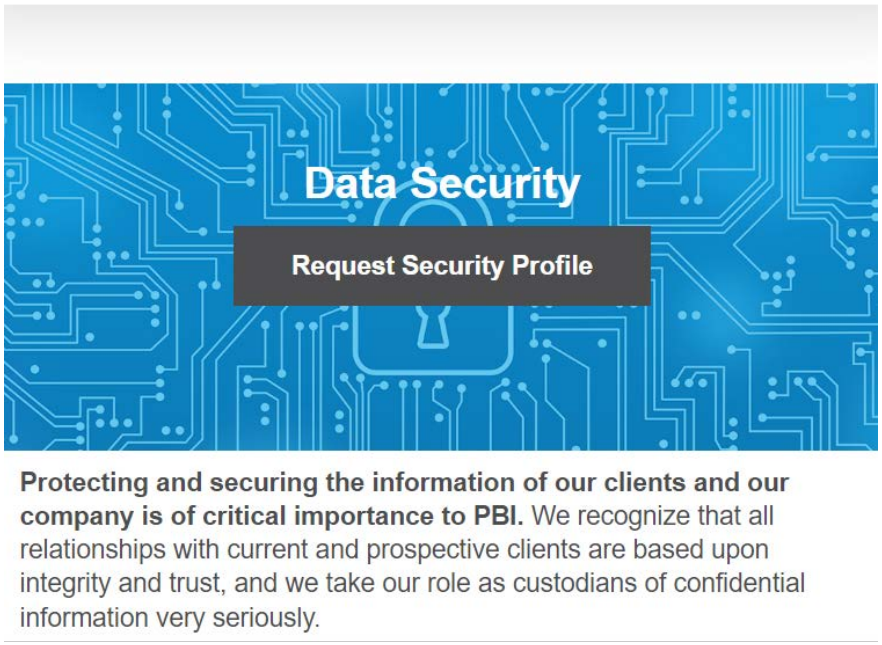
29. PBI is a pension plan "sponsor, administrator, or record keeper" "for thousands of organizations" and pension plans, and one of the many companies that uses PSC's MOVEit service to transfer large amounts of data in the ordinary course of its business and the service it

[4] https://www.tiaa.org/public/support/privacy/privacy-notice (last visited Sept. 11, 2023).

provides to pension plans and other organizations.[5]

30. According to the Notice Letter received by Plaintiff, PBI provides audit and address research services for TIAA.

31. PBI's website also promises consumers that it has robust systems and processes in place to protect and secure their sensitive information:



[5] https://www.pbinfo.com/ (last visited August 1, 2023).

PBI uses a multi-layered approach to protect data securely that includes, but is not limited to the following: implementing secure development practices, including annual training for our IT team, real time scanning of code changes for vulnerabilities, web application firewalls, n-tier application architecture, required security awareness training program for all employees at onboarding and on a regular basis, data loss prevention tools to alert and block transfers of sensitive data, and a consolidated SIEM solution that correlates alerts and events across multiple environments. PBI's data security team manages this multi-layered security architecture by performing over 30 security reviews of quarterly audit checks to test compliance against security policies.

PBI's formalized security program follows the industry-recognized security policy frameworks from the National Institute of Science & Technology (NIST) SP 800-53 and NIST Cybersecurity Framework.

SOC2 Audit and Third-party Security Testing

PBI undergoes an annual SSAE 18 SOC 2, Type II audit by an independent third-party to audit our controls over data confidentiality, integrity, security, and availability.

PBI regularly uses third parties to test and audit our security controls. We conduct monthly and quarterly vulnerability assessments and penetration tests of PBI's internal and external network and application security, and conduct annual application penetration tests.

32. PBI's website also tells consumers that it has systems and process in place to ensure the privacy of their sensitive information obtained over the internet and to prevent identity theft:

9. ONLINE PRIVACY

PBI strives to protect the privacy of personally identifiable information obtained over the Internet and strives to apply the Principles and evolving standards to the online environment.

10. IDENTITY THEFT

PBI strives to prevent the acquisition of information from our products and services for improper purposes, such as identity theft. PBI believes in the importance of notifying individuals who may have had their sensitive personally identifiable information acquired by an unauthorized individual, as appropriate.

33. Furthermore, PBI acknowledges that it has a duty to safeguard Plaintiff's and

Class Members' sensitive PII and PHI because, *inter alia*, PBI's website tells consumers that it has systems in place to protect consumers' sensitive information, and routinely audits those systems to ensure they are compliant with federal regulations and other legislation—as well as industry standards and practices— governing data privacy:

> **8. ACCOUNTABILITY**
>
> PBI supports accountability of information industry standards and practices, responsible and effective federal regulation of the data industry, and legislation governing the practices of all data providers. PBI also supports industry oversight and active engagement with the privacy community. PBI believes that strong privacy and information security protections are vital for an effective and trusted data industry.
>
> **11. COMPLIANCE**
>
> PBI will obtain assessments from an independent auditor, who uses procedures and standards generally accepted in the profession to assess PBI's controls relevant to security, availability, and confidentiality, as appropriate.

34. Discovery will show that through their provision of the foregoing services, PBI obtains possession of customers'—including Plaintiff's and Class Members'—highly sensitive PII. Thus, in the regular course of their business, PBI collects and/or maintains the PII of consumers such as Plaintiff and Class Members. PBI stores this information digitally in the regular course of business.

35. As evidenced by, *inter alia*, their receipt of the notice informing them that their PII were compromised in the Data Breach, Plaintiff's and Class Members' PII was transferred using PSC's MOVEit service and/or they otherwise entrusted to Defendants their PII, from which Defendants profited.

36. Yet, contrary to PBI's website representations—by virtue of Defendants' admissions that they experienced the Data Breach—Defendants did not have adequate measures in place to protect and maintain sensitive PII and PHI entrusted to them. Instead, Defendants'

websites wholly fail to disclose the truth: that Defendants lack sufficient processes to protect the PII and PHI that is entrusted to them.

37. In the course of their relationship, clients, including Plaintiff and Class Members, provided Defendants, directly or indirectly, with at least the following PII:

a. names;

b. gender;

c. dates of birth;

d. Social Security numbers; and

e. addresses.

38. In the course of their ordinary business operations, Defendants are entrusted with safeguarding the sensitive PII of TIAA members.

The Data Breach

39. On or about May 31, 2023, TIAA became aware that PBI, the entity with which TIAA regularly shared PII and which it allowed to maintain the PII of Plaintiff and Class Members, permitted that PII to be accessed by an unauthorized party.

40. In the notice letter sent to Plaintiff, PBI revealed that TIAA had provided Plaintiff's and Class Members sensitive PII to PBI for "audit and address research services." [6] PBI further admitted that—between May 29, 2023 and May 30, 2023—the software it uses to transfer files

[6] *See* August 11, 2023, Data Breach Letter from Pension Benefit Information, LLC (attached as **Exhibit A**).

containing TIAA customer PII "had been exploited by an unauthorized third party" and data containing PII had been downloaded.[7]

41. Absent from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiff and Class Members, who retain a vested interest in ensuring that their PII remains protected.

42. Defendants' Notice Letter admits that Plaintiff's and Class Members' Private Information was accessed without authorization.

Plaintiff Patricia Marshall's Experience

43. As a requisite to receiving financial services, including the provisions of life insurance, from TIAA, Plaintiff provided her Private Information to Defendants and trusted that the information would be safeguarded according to state and federal law.

44. Plaintiff is very careful about sharing her sensitive Private Information, and she has never knowingly transmitted unencrypted sensitive Private Information.

45. Plaintiff stores any documents containing her sensitive Private Information in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts. Had she known Defendants failed to follow basic industry security standards and failed to implement systems to protect her Private Information, she would not have provided that information to Defendants.

46. The Notice Letter dated August 11, 2023 from Defendants notified Plaintiff that their network had been accessed and Plaintiff's Private Information may have been involved in the

[7] *Id.*

Data Breach, which included Plaintiff's name, social security number, gender, date of birth, and address.

47. Furthermore, Defendants directed Plaintiff to be vigilant and to take certain steps to protect her Private Information and otherwise mitigate her damages.

48. As a result of the Data Breach, Plaintiff heeded Defendants' warning and spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice Letter and self-monitoring her 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 Defendants' direction by way of the Data Breach notice where Defendants advised Plaintiff to mitigate her damages by, among other things, reviewing her account statements and monitoring her credit reports.

49. Even with the best response, the harm caused to Plaintiff cannot be undone.

50. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of Plaintiff's Private Information—a form of intangible property that Plaintiff entrusted to Defendants, which was compromised in and as a result of the Data Breach.

51. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

52. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of unauthorized third parties and possibly criminals.

53. In the Notice Letter, Defendants make an offer of 24 months of identity monitoring services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly

face multiple years of ongoing identity theft, medical and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

54. Future identity theft monitoring is reasonable and necessary and such services will include future costs and expenses.

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

The Data Breach Was Eminently Foreseeable

56. At all relevant times, Defendants 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 Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

57. Defendants were, or should have been, fully aware of the unique type and the significant volume of data on their network, amounting to potentially millions of individuals' detailed, personal information and thus the significant number of individuals who would be harmed by the exposure of the unencrypted data.

58. 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."[8]

[8] *See* How to Protect Your Networks from RANSOMWARE, at 3, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last accessed Sept. 12, 2023).

59. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the financial services industry preceding the date of the breach.

60. Indeed, cyberattacks 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, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals… because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[9]

61. Therefore, the increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to anyone in Defendants' industries, including Defendants.

Value of PII

62. The PII of consumers remains of high value to criminals, as evidenced by the prices offered 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.[10] According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an

[9] FBI, Secret Service Warn of Targeted, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbisecret-service-warn-of-targeted-ransomware (last accessed Sept. 12, 2023).

[10] *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 accessed Sept. 12, 2023).

average market value of $120.[11] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[12]

63. The information stolen in the Data Breach—most notably names and Social Security numbers—is difficult, if not impossible, to change. This kind of data, as one would expect, demands a much higher price on the dark web. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information… [is] worth more than 10x on the black market."13

64. Based on the foregoing, the PII 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.

65. 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.

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

67. There is also a robust legitimate market for the type of sensitive information at issue here. Marketing firms utilize personal information to target potential customers, and an entire economy exists related to the value of personal data.

---

[11] *Dark Web Price Index 2021*, Zachary Ignoffo, March 8, 2021, https://www.privacyaffairs.com/dark-web-price-index-2021/ (last accessed Sept. 12, 2023).
[12] *In the Dark*, VPNOverview, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Sept. 12, 2023).
[13] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hackpersonal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Aug. 4, 2023).

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[14]

69. As such, future monitoring of financial and personal records is reasonable and necessary well beyond the two years of protection offered by Defendants.

Defendants Failed to Properly Protect Plaintiff's and Class Members' Private Information

70. Defendants could have prevented this Data Breach by ensuring that the Private Information of Plaintiff and Class Members was properly secured in an encrypted system. Alternatively, Defendants could have destroyed the data, especially for individuals with whom any relationship had ended for a period of time prior to the breach.

71. Defendants' negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendants to protect and secure sensitive data they possess.

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

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

---

[14] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf (last accessed Sept. 12, 2023).

The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[15]

74. The ramifications of Defendants' failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

75. To prevent and detect unauthorized cyber-attacks, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

[15] *See generally Fighting Identity Theft With the Red Flags Rule: A How-To Guide for Business*, FTC, https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business (last accessed Sept. 12, 2023).

- 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.[16]

76. Because Defendants failed to properly protect and safeguard Plaintiff's and Class Members' Private Information, an unauthorized third party was able to access and exfiltrate Plaintiff and Class Members' PII.

Defendants Failed to Comply with FTC Guidelines

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

78. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient 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.[17]

[16] *Id.* at 3-4.
[17] *Protecting Personal Information: A Guide for Business*, FTC (2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed Sept. 12, 2023).

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

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

81. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient 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 clarify the measures businesses take to meet their data security obligations.

82. Defendants failed to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information, constituting an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Defendants Failed To Comply with the Gramm-Leach-Bliley Act

83. TIAA is a financial institution, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

84. The GLBA defines a financial institution as "any institution the business of

which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

85. Defendants collect nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n), and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Defendants were subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1, *et seq*., and is subject to numerous rules and regulations promulgated on the GLBA statutes.

86. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the Consumer Financial Protection Bureau ("CFPB") became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

87. Accordingly, Defendant's conduct is governed by the Privacy Rule prior to December 30, 2011, and by Regulation P after that date.

88. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; C.F.R. §§ 1016.4 and 1016.5.

89. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." C.F.R. § 313.9; 12 C.F.R. § 1016.9.

90. As alleged herein, Defendants violated the Privacy Rule and Regulation P.

91. Upon information and belief, Defendants failed to provide annual privacy notices to clients after their relationship ended, despite retaining these clients' PII and storing that PII on Defendants' network systems.

92. Defendants failed to adequately inform that they were storing and/or sharing, or would store and/or share, the customers' PII on an insecure platform, accessible to unauthorized parties from the internet, and would do so after the customer relationship ended.

93. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract

to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4.

94. As alleged herein, Defendants violated the Safeguard Rule.

95. Defendants failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information and failed to monitor the systems of its IT partners or verify the integrity of those systems.

96. Defendants violated the GLBA and its own policies and procedures by sharing the PII of Plaintiff and Class Members with a non-affiliated third party without providing Plaintiff and Class Members (a) an opt-out notice and (b) a reasonable opportunity to opt out of such disclosure.

Defendants Failed to Comply with Industry Standards

97. As shown 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.

98. Several best practices have been identified that at a minimum should be implemented by financial services companies like Defendants, including, but not limited to: educating all employees; utilizing 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.

99. Other best cybersecurity practices that are standard for financial services companies 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; and training staff regarding critical points.

100. Defendants 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.

101. The foregoing frameworks are existing and applicable industry standards in the financial services industry, and Defendants failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

102. Upon information and belief, Defendants failed to comply with one or more of the foregoing industry standards.

Defendants' Negligent Acts & Breaches

103. Defendants participated in and controlled the process of gathering the Private Information from Plaintiff and Class Members.

104. Defendants therefore assumed and otherwise owed duties and obligations to Plaintiff and Class Members to take reasonable measures to protect the information, including the duty of oversight, training, instruction, testing of the data security policies and network systems. Defendants breached these obligations to Plaintiff and Class Members and/or were otherwise negligent because they failed to properly implement data security systems and policies that would have adequately safeguarded Plaintiff's and Class Members' Private Information.

COMMON INJURIES & DAMAGES

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

106. Due to the Data Breach, and the foreseeable consequences of Private Information 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 of value of their Private Information; and (i) the continued risk to their Private Information, which remains in Defendants' possession, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

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

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

108. 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.

109. 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.

110. The dark web is an unindexed layer of the internet that requires special software or authentication to access.[18] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[19] This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

111. 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.[20] The digital character of PII stolen in data breaches lends itself to dark web transactions

---

[18] Experian, *What Is the Dark Web?*, https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last accessed Sept. 12, 2023).

[19] *Id.*

[20] Microsoft 365, *What is the Dark Web*?, https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web (last accessed Sept. 12, 2023).

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.[21] As Microsoft warns, "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[22]

112. Social Security numbers, for example, are among the worst kinds of personal information to have stolen because they may be put to numerous serious fraudulent uses and are difficult for an individual to change.

113. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[23]
>
> 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.

---

21 *Id.*

22 *Id.*

23 Social Security Administration, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Sept. 12, 2023).

114. 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."[24]

115. 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.[25]

116. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[26]

117. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[27] But Defendants did not rapidly report to Plaintiff and the Class that their Private Information had been stolen.

---

[24] 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 accessed Sept. 12, 2023).
[25] Social Security Administration, *Identity Theft and Your Social Security Number*, at *1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Sept. 12, 2023).
[26] https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last accessed Sept. 12, 2023).
[27] *Id.*

118. 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.

119. 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.

120. 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.

121. 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 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."[28]

122. 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.

[28] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last accessed Sept. 12, 2023).

123. 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.[29]

124. 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.[30]

125. Defendants' 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 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 Identity Theft and Fraud

126. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the

[29] *See generally* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed Sept. 12, 2023).

[30] *See, e.g.*, https://www.ftc.gov/news-events/news/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices (last accessed Sept. 12, 2023).

dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet, the resource and asset of time has been lost.

127. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, as Defendants' Notice instructs them, "review[] your account statements and monitor[] your free credit reports for suspicious activity."

128. 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—which may take years to discover and detect—and filing police reports.

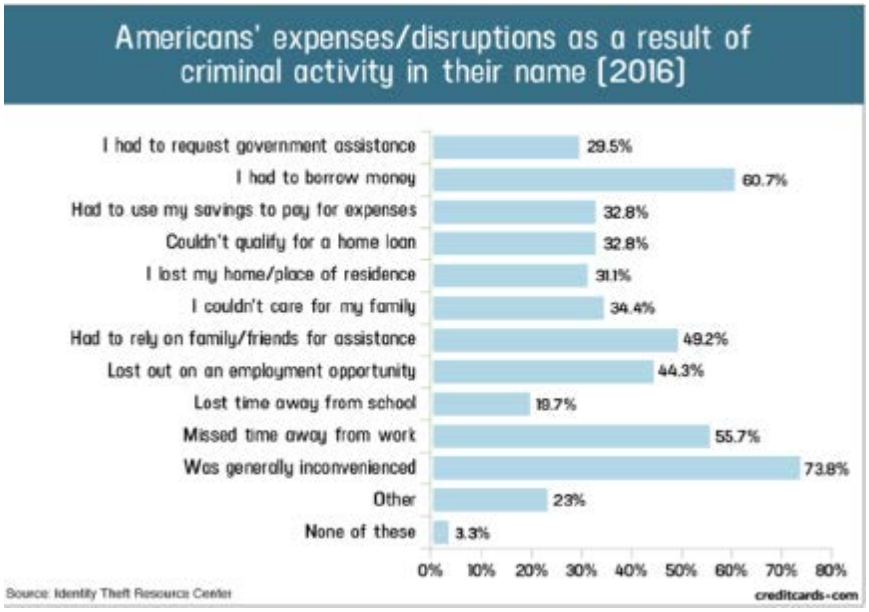
129. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office, who released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[31]

130. 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

[31] *See* United States Government Accountability Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf (last accessed Sept. 12, 2023).

credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[32]

131. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[33]



132. In the event that Plaintiff and Class Members experience actual identity theft and fraud, the GAO Report noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[34] 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

[32] *See* FTC, IdentityTheft.com, https://www.identitytheft.gov/Steps (last accessed Sept. 12, 2023).
[33] Jason Steele, *Credit Card and ID Theft Statistics*, Oct. 24, 2017, https://web.archive.org/web/20171215215318/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last accessed Sept. 12, 2023).
[34] *See supra* note 28.

their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[35]

Diminution of Value of the Private Information

133. PII is a valuable property right.[36] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

134. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[37]

135. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[38] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[39] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[40]

---

[35] *See* https://www.identitytheft.gov/Steps.

[36] *See, e.g.*, John T. Soma, *et al*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[37] *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 accessed Sept. 12, 2023).

[38] *See* David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last accessed Sept. 12, 2023).

[39] *See* https://datacoup.com/ (last accessed Sept. 12, 2023).

[40] Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last accessed Sept. 12, 2023).

136. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release onto the Dark Web, where it may soon be available and holds significant value for the threat actors.

137. To date, Defendants have done little to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach – Defendants have only offered two years of inadequate identity monitoring services through Kroll—and only to some Class Members—despite Plaintiff and all Class Members being at risk of identity theft and fraud for the foreseeable future. Defendants have also offered "$1 Million Identity Fraud Loss Reimbursement" to some Class Members, but not to Plaintiff or many others.

138. The two years of credit monitoring and purported "$1 Million" reimbursement offered to some persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud. Defendants also place the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for that service, as opposed to automatically enrolling all victims of this Data Breach.

139. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information, 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 Private Information for identity theft crimes – e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

140. 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 Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[41]

141. 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.

142. 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.[42] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

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

---

[41] *See supra* note 28, GAO Report, at p. 29.

[42] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds* (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 accessed Sept. 12, 2023).

144. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendants' 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 Defendants' failure to safeguard their Private Information.

Injunctive Relief Is Necessary to Protect Against Future Data Breaches

145. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendants, 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 Private Information is not accessible online and that access to such data is password protected.

CLASS ACTION ALLEGATIONS

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

147. Specifically, Plaintiff proposes the following classes (collectively, the "Class"):

(1) PSC Nationwide Class: All persons whose Private Information was compromised in the MOVEit data breach.

   (a) PSC Vermont Class: All residents of Vermont whose Private Information was compromised in the MOVEit data breach.

(2) PBI Nationwide Class: All persons whose Private Information was compromised on PBI's platform and/or systems in the MOVEit data breach.

   (a) PBI Vermont Class: All residents of Vermont whose Private Information was compromised on PBI's platform and/or systems in the MOVEit data breach.

(3) TIAA Nationwide Class: All persons whose Private Information was compromised in the MOVEit data breach where such Private Information was

obtained from or hosted by TIAA.

(a) TIAA Vermont Class: All residents of Vermont whose Private Information was compromised in the MOVEit data breach where such Private Information was obtained from or hosted by TIAA.

The foregoing state-specific classes are collectively referred to as the "State Classes" and the foregoing nationwide classes are collectively referred to as the "Nationwide Classes."

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

149. Plaintiff reserves the right to modify or amend the definition of the proposed Classes before the Court determines whether certification is appropriate.

150. Numerosity, Fed. R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are nearly 2.3 million individuals whose Private Information may have been improperly accessed in the Data Breach, and each Class is apparently identifiable within Defendant's records.[43]

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

[43] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/ed67df63-aced-4ecb-91ce-602c7e34c83a.shtml (last visited Sept. 11, 2023).

a) Whether and to what extent Defendants had a duty to protect the Private Information of Plaintiff and Class Members;
b) Whether Defendants had duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;
c) Whether Defendants had duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;
d) Whether Defendants failed to adequately safeguard the Private Information of Plaintiff and Class Members;
e) Whether and when Defendants actually learned of the Data Breach;
f) Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;
g) Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;
h) Whether both Defendants 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 Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;
j) Whether Defendants violated the consumer protection statutes invoked herein;
k) Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendants' wrongful conduct;
l) Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and
m) 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.

152. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

153. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy. Defendants' policies challenged herein apply to and

affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

154. Adequacy of Representation, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Clasess. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Classes and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

155. Superiority, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like 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.

156. 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 Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

157. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, uniform methods of data collection, 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.

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

159. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the Private Information of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

160. Further, Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

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

a. Whether Defendants owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendants breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendants on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendants breached the implied contract;

f. Whether Defendants adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

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

h. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members; and

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

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(*On Behalf of Plaintiff, the State Classes, and the Nationwide Classes, Against All Defendants*)

162. Plaintiff and the Class reallege and incorporate by reference all other paragraphs of the Complaint as if fully set forth herein.

163. Defendants owed to Plaintiff and the Class a duty of reasonable care in handling and using this information and securing and protecting the information from being stolen, accessed, and misused by unauthorized parties. This duty extended to any vendor selected by Defendants to be entrusted with the sensitive data of Plaintiff and Class Members.

164. Defendants owed this duty to Plaintiff and the other Class Members because Plaintiff and the other Class Members compose a well-defined, foreseeable, and probable class of individuals whom Defendants should have been aware that Plaintiff and Class Members could be injured by Defendants' inadequate security protocols. Defendants actively solicited clients who entrusted Defendants with Plaintiff's and the other Class Members' PII when obtaining and using Defendants' services. To facilitate these services, Defendants used, handled, gathered, and stored the PII of Plaintiff and the other Class Members. Thus, Defendants had a duty to act reasonably in protecting the PII of their clients.

165. The duty included obligations to take reasonable steps to prevent disclosure of Private Information, and to safeguard the information from theft. Defendants' breached these duties by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII entrusted to them—including Plaintiff's and Class Members' PII.

166. Defendants' duty of care arose as a result of the special relationship that existed between Defendants and their clients, which is recognized by laws and regulations including but not limited to the FTC Act, and common law. Defendants were in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

167. Defendants had a duty 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.

168. Defendants breached their duties, pursuant to the FTC Act, GLBA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' PII.

169. Defendants violated Section 5 of the FTC Act and GLBA by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendants' 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.

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

171. Defendants' violations of Section 5 of the FTC Act and the GLBA constitute negligence.

172. Defendants' 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 Defendants are bound by industry standards to protect confidential Private Information that they either acquire, maintain, or store.

173. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information, as alleged and discussed above.

174. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' Private Information would result in injury to Plaintiff and 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.

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

176. The imposition of a duty of care on Defendants to safeguard the Private Information they maintained is appropriate because any social utility of Defendants' conduct is outweighed by the injuries suffered by Plaintiff and Class Members as a result of the Data Breach.

177. But for Defendants' negligent conduct or breach of the above-described duties owed to Plaintiff and Class Members, their PII would not have been compromised. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding, securing, and protecting such PII.

178. As a direct and proximate result of Defendants' negligence, Plaintiff and Class Members are at a current and ongoing risk of identity theft, and Plaintiff and Class Members sustained compensatory damages including: (a) invasion of privacy; (b) financial "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) financial "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) diminution of value of their Private Information; (h) future costs of identity theft monitoring; (i) anxiety, annoyance and nuisance, and (j) the continued risk to their Private Information, which remains in Defendants' possession, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

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

COUNT II
NEGLIGENCE *PER SE*
(*On Behalf of Plaintiff, the State Classes, and the Nationwide Classes, Against All Defendants*)

180. Plaintiff and the Class reallege and incorporate by reference all preceding paragraphs as if fully set forth herein.

181. Defendants' duties arise from, inter alia, Section 5 of the FTC Act ("FTCA"), 15U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to employ reasonable measures to protect and secure PII.

182. Defendants' duty to use reasonable security measures also arose under the GLBA, under which they were required to protect the security, confidentiality, and integrity of client information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

183. Defendants violated Section 5 of the FTCA and the GLBA by failing to use reasonable measures to protect Plaintiff's and all other Class Members' PII and comply with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII they obtain and store, and the foreseeable consequences of a data breach involving PII including, specifically, the substantial damages that would result to Plaintiff and the other Class Members.

184. Defendants' violations of Section 5 of the FTCA and the GLBA constitute negligence *per se*.

185. Plaintiff and Class Members are within the class of persons that Section 5 of the FTCA and the GLBA were intended to protect.

186. The harm occurring as a result of the Data Breach is the type of harm Section 5 of the FTCA and the GLBA were intended to guard against.

187. It was, or should have been, reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

188. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of Defendants' violations of Section 5 of the FTCA and the GLBA.

189. Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention,

detection, and recovery from unauthorized use of their PII; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; (vii) loss of value of their PII, for which there is a well-established national and international market; and (viii) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF FIDUCIARY DUTY
(*On Behalf of Plaintiff, the State Classes, and the Nationwide Classes, Against All Defendants*)

190. Plaintiff and the Class reallege and incorporate by reference all other paragraphs of the Complaint as if fully set forth herein.

191. In providing their Private Information to Defendants, Plaintiff and Class Members justifiably placed a special confidence in Defendants to act in good faith and with due regard for the interests of Plaintiff and Class Members to safeguard and keep confidential that Private Information.

192. Defendants accepted the special confidence Plaintiff and Class Members placed in it, as evidenced by their assertion that they are committed to protecting the privacy of Plaintiff's personal information as included in the Data Breach notification letter.

193. In light of the special relationship between Defendants, Plaintiff, and Class Members, whereby Defendants became guardians of Plaintiff and Class Members' Private Information, Defendants became fiduciaries by undertaking the guardianship of the Private Information, to act primarily for the benefit of their clients, including Plaintiff and Class Members, for the safeguarding of Plaintiff and Class Members' Private Information.

194. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their client relationships, in particular, to keep secure the Private Information of their customers.

195. Defendants breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' PII, failing to comply with the data security guidelines set forth by Section 5 of the FTCA and the GLBA, and otherwise failing to safeguard Plaintiff's and Class Members' PII that they collected.

196. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to:

a. Actual identity theft;

b. The compromise, publication, and/or theft of their Private Information;

c. Out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information;

d. Lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft;

e. The continued risk to their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in their continued possession;

f. Future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and

g. The diminished value of the services they paid for and received.

197. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiff and Class Members will suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT IV
UNJUST ENRICHMENT
(*On Behalf of Plaintiff, the State Classes, and the Nationwide Classes, Against All Defendants*)

198. Plaintiff and the Class reallege and incorporate by reference all other paragraphs of the Complaint as if fully set forth herein.

199. Plaintiff pleads this claim in the alternative to her breach of implied contract claim below in Count VI.

200. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they provided Defendants with their Private Information.

201. In exchange, Plaintiff and Class Members should have received from Defendants data storage that was compliant with and maintained in accordance with Defendants' pre-existing duties to secure such information under federal law and industry standards and were entitled to have Defendants protect their Private Information with adequate security.

202. Defendants knew that Plaintiff and Class Members conferred a benefit on them and accepted or retained that benefit. Defendants profited from Plaintiff's and Class Members' Private Information for business purposes.

203. Defendants failed to secure Plaintiff's and Class Members' Private Information and therefore, did not provide full compensation for the benefit the Plaintiff and Class Members' Private Information provided.

204. Defendants acquired the Private Information through inequitable means as they failed to disclose the inadequate security practices previously alleged.

205. If Plaintiff and Class Members had known that Defendants would not secure their Private Information using adequate security, they would not have provided their information to Defendants.

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

207. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class Members conferred on it.

208. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiff and Class Members overpaid for the use of Defendants' services.

COUNT V
VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW § 349
N.Y. Gen. Bus. Law § 349*, et seq.*
(*On Behalf of Plaintiff, the State Classes, and the Nationwide Classes, Against All Defendants*)

209. Plaintiff and the Class reallege and incorporate by reference all other paragraphs of the Complaint as if fully set forth herein.

210. New York Deceptive Trade Practices Act, N.Y. Gen. Bus. Law § 349, prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in the state of New York.

211. By reason of the conduct alleged herein, Defendants engaged in unlawful practices within the meaning of the N.Y. Gen. Bus. Law § 349. The conduct alleged herein is a "business

practice" within the meaning of the N.Y. Gen. Bus. Law § 349, and the deception occurred within New York State.

212. Plaintiff and Class Members would not have provided their Private Information if they had been told or knew that Defendants failed to maintain sufficient security thereof, and its inability to safely store Plaintiff's' and Class Members' Private Information.

213. As alleged herein in this Complaint, Defendants engaged in the unfair or deceptive acts or practices in the conduct of consumer transactions in violation of N.Y. Gen. Bus. Law § 349, including but not limited to:

- Representing that their services were of a particular standard or quality that they knew or should have known were of another;
- Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' Private Information, which was a direct and proximate cause of the Data Breach;
- Failing to identify foreseeable security and privacy risks, and remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;
- Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Private Information, including duties imposed by the FTCA, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;
- Misrepresenting that they would protect the privacy and confidentiality of Plaintiff's and Class Members' Private Information, including by implementing and maintaining reasonable security measures;
- Omitting, suppressing, and concealing the material fact that they did not reasonably or adequately secure Plaintiff's and Class Members' Private Information; and
- Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' Personal Information, including duties imposed by the FTCA, 15 U.S.C. §

45, which was a direct and proximate cause of the Data Breach.

214. Defendants' representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendants' data security and ability to protect the confidentiality of consumers' Private Information.

215. Such acts by Defendants are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer providing his or her Private Information to Defendants. Said deceptive acts and practices are material. The requests for and use of such Private Information in New York through deceptive means occurring in New York were consumer-oriented acts and thereby falls under the New York consumer fraud statute, N.Y. Gen. Bus. Law § 349.

216. In addition, Defendants' failure to secure consumers' Private Information violated the FTCA and therefore violates N.Y. Gen. Bus. Law § 349.

217. The aforesaid conduct violated N.Y. Gen. Bus. Law § 349, in that it is a restraint on trade or commerce.

218. Defendants' violations of N.Y. Gen. Bus. Law § 349 have an impact and general importance to the public, including the people of New York. Thousands of New Yorkers have had their Private Information stored on Defendants' electronic databases, many of whom have been impacted by the Data Breach.

219. As a direct and proximate result of these deceptive trade practices, Plaintiff and Class Members are entitled to judgment under N.Y. Gen. Bus. Law § 349, to enjoin further violations, to recover actual damages, to recover the costs of this action (including reasonable attorneys' fees), and such other relief as the Court deems just and proper.

220. On information and belief, Defendant TIAA oversaw its data privacy program complained of herein from New York, and its communications and other efforts to hold participant data largely emanated from New York.

221. Most, if not all, of the alleged misrepresentations and omissions by TIAA that led to inadequate measures to protect patient information occurred within or were approved within New York.

222. TIAA's implied and express representations that it would adequately safeguard Plaintiff's and Class Members' Private Information constitute representations as to the particular standard, quality, or grade of services that such services did not actually have (as the services were of another, inferior quality), in violation of N.Y. Gen. Bus. Law § 349.

223. Accordingly, Plaintiff, on behalf of herself and Class Members, brings this action under N.Y. Gen. Bus. Law § 349 to seek such injunctive relief necessary to enjoin further violations and recover costs of this action, including reasonable attorneys' fees and other costs.

COUNT VI
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff, the State Classes, and the Nationwide Classes, Against All Defendants)

224. Plaintiff and the Class reallege and incorporate by reference all other paragraphs of the Complaint as if fully set forth herein.

225. Plaintiff and Class Members were required to provide their Private Information to Defendants as a condition of their use of TIAA's services.

226. Plaintiff and Class Members paid money to Defendants in exchange for services, along with Defendants' promise to protect their Private Information from unauthorized access and disclosure.

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

228. When Plaintiff and Class Members provided their PII to Defendants, they entered into implied contracts with Defendants pursuant to which Defendants agreed to reasonably protect such information.

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

230. Plaintiff and Class Members would not have entrusted their Private Information to Defendants in the absence of the implied contract between them and Defendants to keep their information reasonably secure, including monitoring their computer systems and networks and adopting reasonable data security measures.

231. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendants.

232. Defendants breached their implied contracts with Class Members by failing to safeguard and protect their Private Information and in failing to implement and maintain security

protocols and procedures to protect Plaintiff's and Class Members' PII in a manner that complies with applicable laws, regulations, and industry standards.

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

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

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

COUNT VII
DECLARATORY AND INJUNCTIVE RELIEF
(*On Behalf of Plaintiff, the State Classes, and the Nationwide Classes, Against All Defendants*)

236. Plaintiff and the Class reallege and incorporate by reference all other paragraphs of the Complaint as if fully set forth herein.

237. Plaintiff pursues this claim under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq*.

238. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

239. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class Members' Private Information, and whether Defendants are currently

maintaining data security measures adequate to protect Plaintiff and Class Members from future data breaches that compromise their Private Information. Plaintiff and the Class remain at imminent risk that further compromises of their Private Information will occur in the future.

240. The Court should also issue prospective injunctive relief requiring Defendants to employ adequate security practices consistent with law and industry standards to protect clients' and customers' Private Information.

241. Defendants still possess the Private Information of Plaintiff and the Class.

242. To Plaintiff's knowledge, Defendants have made no announcement that they have changed their data storage or security practices relating to the Private Information, beyond the vague claim in the Notice Letter that it is the steps it took to "patch servers" and "assess the security of our systems."

243. To Plaintiff's knowledge, Defendants have made no announcement or notification that they have remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

244. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach. The risk of another such breach is real, immediate, and substantial.

245. As described above, actual harm has arisen in the wake of the Data Breach regarding Defendants' contractual obligations and duties of care to provide security measures to Plaintiff and Class Members. Further, Plaintiff and Class members are at risk of additional or further harm due to the exposure of their Private Information and Defendant's failure to address the security failings that led to such exposure.

246. There is no reason to believe that Defendants' employee training and security measures are any more adequate now than they were before the breach to meet Defendants' contractual obligations and legal duties.

247. The hardship to Plaintiff and Class Members if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if another data breach occurs, Plaintiff and Class Members will likely continue to be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

248. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the additional injuries that would result to Plaintiff and Class.

249. Plaintiff and Class Members, therefore, seek a declaration (1) that Defendants' existing data security measures do not comply with their contractual obligations and duties of care to provide adequate data security, and (2) that to comply with contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to, the following:

a. Ordering that Defendants engage internal security personnel to conduct testing, including audits on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train their security personnel and employees regarding any new or modified data security policies and procedures;

d. Ordering that Defendants purge, delete, and destroy, in a reasonably secure manner, any Private Information not necessary for their provision of services;

e. Ordering that Defendants conduct regular database scanning and security checks; and

f. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel and employees how to safely share and maintain highly sensitive personal information, including but not limited to, client personally identifiable information.

PRAYER FOR RELIEF

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

A. For an Order certifying the Class, and appointing Plaintiff and her Counsel to represent the Class;

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

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

D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

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

F. For prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

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

Date: June 12, 2024

Respectfully Submitted,

By: */s/ Kristen A. Johnson*
Kristen A. Johnson (BBO# 667261)
HAGENS BERMAN SOBOL SHAPIRO LLP
1 Faneuil Hall Square, 5th Fl.
Boston, MA 02109
Tel: (617) 482-3700
Fax: (617) 482-3003
kristenj@hbsslaw.com

Plaintiffs' Liaison & Coordinating Counsel

David S. Almeida
New York Bar No. 3056520
Matthew J. Langley
New York Bar No. 4831749
Elena A. Belov
New York Bar No. 4080891
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
(312) 576-3024
david@almeidalawgroup.com
elena@almeidalawgroup.com

Counsel for Plaintiff & the Class

E. Michelle Drake
BERGER MONTAGUE, PC
1229 Tyler St., NE, Ste. 205
Minneapolis, MN 55413
Tel: (612) 594-5933
Fax: (612) 584-4470
emdrake@bm.net

Gary F. Lynch
LYNCH CARPENTER, LLP
1133 Penn Ave., 5th Fl.
Pittsburgh, PA 15222
Tel: (412) 322-9243
Fax: (412) 231-0246
Gary@lcllp.com

Douglas J. McNamara
COHEN MILSTEIN SELLERS & TOLL PLLC
1100 New York Ave. NW, 5th Fl.
Washington, DC 20005
Tel: (202) 408-4600
dmcnamara@cohenmilstein.com

Karen H. Riebel
LOCKRIDGE GRINDAL NAUEN PLLP
100 Washington Ave. S., Ste. 2200
Minneapolis, MN 55401
Tel: (612) 339-6900
Fax: (612) 612-339-0981
khriebel@locklaw.com

Charles E. Schaffer
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Ste. 500
Philadelphia, PA 19106
Tel: (215) 592-1500
Fax: (215) 592-4663
cshaffer@lfsblaw.com

Plaintiffs' Lead Counsel

CERTIFICATE OF SERVICE

I hereby certify that, on this date, the foregoing document was served by filing it on the Court's CM/ECF system, which will automatically send a notification of such filing to all counsel of record via electronic mail.

Dated: June 12, 2024

/s/ Kristen Johnson
Kristen Johnson