IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

ERIC GIANNINI, individually and on behalf of all others similarly situated, Plaintiff, v. TRANSAMERICA RETIREMENT SOLUTIONS, LLC, Defendant.	)	**Case No.:** 7:21-cv-10282 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Eric Giannini ("Plaintiff"), individually and on behalf of all others similarly situated, through the undersigned counsel, hereby alleges the following against Defendant Transamerica Retirement Solutions, LLC ("Transamerica" or "Defendant").

NATURE OF THE ACTION

1. This is a class action for damages with respect to Transamerica Retirement Solutions, LLC, for its failure to exercise reasonable care in securing and safeguarding their client's sensitive information—including names, addresses, Social Security Numbers, and retirement fund contribution amounts, collectively known as personally identifiable information ("PII" or "Private Information").

2. This class action is brought on behalf of individual retirement fund plan participants who used Transamerica's services and had their sensitive PII accessed by unauthorized parties because of a lapse in network security in or around June of 2021 (the "Data Breach").

3. The Data Breach affected retirement plan beneficiaries who use Transamerica's services in multiple states.

4. Transamerica reported to Plaintiff that information compromised in the Data Breach included his PII.

5. Plaintiff was not notified until October 8, 2021, nearly four months after his information was first accessed.

6. Plaintiff has experienced a number of harms as a result of the Data Breach incident since Transamerica's systems were accessed, including the misuse of his identifying information for fraudulent purchases.

7. As a result of the Data Breach, Plaintiff and other class members will continue to experience various types of misuse of their PII in the coming years, including but not limited to unauthorized credit card charges, unauthorized access to email accounts, and other fraudulent use of their financial information.

8. There has been no assurance offered from Transamerica that all personal data or copies of data have been recovered or destroyed. Transamerica offered Equifax credit monitoring, which does not guarantee the security of Plaintiff's information. To mitigate further harm, Plaintiff chose not to disclose any more information to receive these services connected with Transamerica.

9. Accordingly, Plaintiff asserts claims for negligence, breach of contract, breach of implied contract, breach of fiduciary duty, and violations of New York General Business Law § 349.

PARTIES

A. Plaintiff Eric Giannini

10. Plaintiff Eric Giannini is a resident of Sacramento, California, and brings this action in his individual capacity and on behalf of all others similarly situated. Mr. Giannini's retirement account through his former employer has been administrated by Transamerica since February of 2019. In maintaining his information, Defendant expressly and impliedly promised to safeguard Plaintiff Giannini's PII. Defendant, however, did not take proper care of Mr. Giannini's PII, leading to its exposure as a direct result of Defendant's inadequate security measures. In October of 2021, Plaintiff Giannini received a notification letter from Defendant stating that his PII was taken, which included Mr. Giannini's "name, address, Social Security number, and figures related to retirement plan distributions and tax information."

11. The letter also offered two years of credit monitoring through Equifax, which was and continues to be ineffective for Giannini and other class members. The Equifax credit monitoring would have shared Mr. Giannini's information with third parties and could not guarantee complete privacy of his sensitive PII.

12. In the months and years following the Data Breach, Mr. Giannini and the other class members will experience a slew of harms as a result of Defendant's ineffective data security measures. Some of these harms will include fraudulent charges, requests for services taken out in beneficiaries' names, and targeted advertising without client consent.

13. These harms are not just theoretical. Mr. Giannini has already experienced a number of fraudulent purchase requests and spam calls in his name after the Data Breach, which will negatively affect his finances in the future.

14. Plaintiff Giannini greatly values his privacy, especially in the administration of his finances, and would not have paid the amount that he did for retirement plan administration services if he had known that his information would be maintained using inadequate data security systems.

B. Defendant

15. Defendant Transamerica Retirement Solutions, LLC is a retirement plan administration company which operates nationally, including in California. Transamerica registered its headquarters at 440 Mamaroneck Avenue, Harrison, New York 10528. Transamerica's corporate policies and practices, including those used for data privacy, are established in, and emanate from the state of New York.

JURISDICTION AND VENUE

16. The Court has jurisdiction over Plaintiff's claims under 28 U.S.C. § 1332(d)(2) ("CAFA"), because (a) there are 100 or more class members, (b) at least one Class member is a citizen of a state that is diverse from Defendant's citizenship, and (c) the matter in controversy exceeds $5,000,000, exclusive of interest and costs.

17. The Court has personal jurisdiction over Defendant because Defendant's principal place of business is located in this District.

18. Venue is proper in this district under 28 U.S.C. § 1391(b)(1) because Defendant maintains its principal place of business in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events or omissions giving rise to the Class's claims also occurred in this District.

FACTS

19. Defendant provides retirement planning solutions to hundreds of employers, with thousands of plan participants in California and millions of plan participants across the country. As part of its business, Defendant was entrusted with, and obligated to safeguard and protect the Private Information of Plaintiff and the Class in accordance with all applicable law.

20. In June of 2021, Defendant first learned of an incident in which changes to its network settings allowed unauthorized access of customer and plan participants' Private Information including names, addresses, Social Security numbers, financial account numbers, and other confidential billing information. Defendant sent the following notice letter template to a number of state data breach reporting agencies:[1]

> Notice of Data Breach
>
> We at Transamerica Retirement Solutions, LLC ("Transamerica") are writing to inform you of an information breach involving some of your personal information that occurred in early June 2021. This letter offers credit monitoring services and information to help protect against the potential for identity theft.
>
> What Information Was Involved
>
> The information that may have been accessed included your name, address, Social Security number, date of birth, and financial details related to retirement plan contributions.
>
> What We Are Doing
>
> When we learned of the incident, we promptly launched an investigation led by counsel. Although we have completed our investigation and found no evidence that your information was misused or further disclosed, we have arranged to provide you with two (2) years of identity monitoring service at our expense (see details below) to assist you in protecting your information.

[1] Transamerica Retirement Solutions, *Notice of Data Breach*, OFFICE OF MASS. ATTN'Y GENERAL (Aug. 8, 2021), https://www.mass.gov/doc/assigned-data-beach-number-21967-transamerica-retirement-solutions-llc/download [hereinafter *Data Breach Notice*].

What You Can Do

We recommend that you take some simple and no-cost steps to help protect against the possibility of identity theft.

We encourage you to be vigilant with respect to carefully reviewing any account/policy statements and your credit reports. You should promptly report any suspicious activity or suspected identity theft to us and to proper law enforcement authorities, including your local law enforcement agency or your state's attorney general. We encourage you to enroll in the complimentary identity theft protection service that we have arranged for you. If you wish to receive this service, please see the enclosed instructions on how to enroll, along with Activation Code []
Even if you do not register for the credit monitoring service, we recommend that you periodically obtain your credit report from one or more of the national credit reporting companies listed in the attached Reference Guide.

You may also contact the Federal Trade Commission ("FTC") or the national credit reporting agencies to learn about preventing identity theft and to obtain additional information on identity theft, fraud alerts and security freezes.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
http://www.ftc.gov/idtheft/

We apologize for any inconvenience this incident may cause. If you have questions or concerns, please do not hesitate to contact us directly at . . .

Sincerely,

Transamerica

21. Upon learning of the Data Breach in June 2021, Defendant investigated. Although Defendant has not provided an estimate of how many plan participants were affected by the Data

Breach, Defendant reported that the incident affected plan participants in multiple states including California, Montana, Massachusetts, and Vermont.[2]

22. In August of 2021 Defendant announced that it first learned of suspicious activity that allowed on ore more unauthorized parties to access their systems through a systems configuration change that left sensitive data exposed. The 2021 Notice disclosed that these changes allowed unauthorized administrators of other retirement plans to view sensitive participant information.

23. Defendant offered no explanation for the delay between the initial discovery of the Breach and the belated notification to affected customers, which resulted in Plaintiff and class members suffering harm they otherwise could have avoided had a timely disclosure been made.

24. Transamerica's notice of Data Breach was not just untimely but woefully deficient, failing to provide basic details, including but not limited to, how unauthorized parties accessed its networks, whether the information was encrypted or otherwise protected, how it learned of the Data Breach, whether the breach occurred system-wide, whether servers storing information were accessed, and how many plan participants were affected by the Data Breach. Even worse, Transamerica offered only two years of identity monitoring for Plaintiff and class members, which required their disclosure of additional PII with which Transamerica had just demonstrated it could not be trusted.

25. Plaintiff and class members' PII is likely for sale to criminals on the dark web, meaning that unauthorized parties have accessed and viewed Plaintiff's and class members'

[2] Various states require that data breach incidents affecting citizens within that state be reported to the attorney general's office within a reasonable period of time after the breach. Defendant sent notice of the Data Breach to several states and its generic notice letter is recorded in multiple state attorneys general consumer protection data breach portals. *See, e.g., id.*

unencrypted, unredacted information, including names, addresses, email addresses, dates of birth, Social Security numbers, member ID numbers, employer names, plan numbers, and more.

26. The Breach occurred because Defendant failed to take reasonable measures to protect the Personal Identifiable Information it collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this release of information, despite repeated warnings to insurance companies and retirement administrators about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past.

27. Defendant disregarded the rights of Plaintiff and class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff and class members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and class members was compromised through unauthorized access. Plaintiff and class members have a continuing interest in ensuring that their information is and remains safe.

A. Defendant's Privacy Promises

28. Transamerica made, and continues to make, various promises to its customers, including Plaintiff, that it will maintain the security and privacy of their Private Information.

29. In its Notice of Privacy Practices, which was updated for 2021, and therefore applicable to Plaintiff, Defendant stated under a section bolded and titled "Protecting Your Data," the following:[3]

> We maintain appropriate controls to limit access to data to persons who need access to it. These persons access your data so that they can do their jobs or provide products and services to you. We train our workforce to properly handle data. In addition, we maintain other physical, technical, and administrative or procedural safeguards to protect your data.

30. Transamerica describes how it may use and disclose financial information for each category of uses or disclosures, none of which provide it a right to expose plan participants' Private Information in the manner it was exposed to unauthorized third parties in the Data Breach.

31. By failing to protect Plaintiffs' and class members' Private Information, and by allowing the Data Breach to occur, Transamerica broke these promises to Plaintiff and class members.

B. Defendant Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Customer's Private Information

32. Transamerica acquires, collects, and stores a massive amount of its customers' protected PII, including financial information and other personally identifiable data.

[3] *Notice of Privacy Practices (Retirement)*, TRANSAMERICA (Apr. 30, 2021), https://www.transamerica.com/sites/default/files/files/e070d/TRS421-PDF.pdf

33. As a condition of engaging in financial and insurance-related services, Transamerica requires that these customers entrust them with highly confidential Private Information.

34. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and class members' Private Information, Transamerica assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and class members' Private Information from disclosure.

35. Defendant had obligations created by industry standards, common law, and representations made to class members, to keep class members' Private Information confidential and to protect it from unauthorized access and disclosure.

36. Defendant failed to properly safeguard class members' Private Information, allowing hackers to access their Private Information.

37. Plaintiff and class members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant and any of its affiliates would comply with their obligation to keep such information confidential and secure from unauthorized access.

38. Prior to and during the Data Breach, Defendant promised customers that their Private Information would be kept confidential.

39. Defendant's failure to provide adequate security measures to safeguard customers' Private Information is especially egregious because Defendant operates in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to customers' highly confidential Private Information.

40. In fact, Defendant has been on notice for years that Plaintiff's and all other Class members' PII was a target for malicious actors. Despite such knowledge, Transamerica failed to implement and maintain reasonable and appropriate security measures to protect Plaintiff's and Class members' PII from unauthorized access Transamerica should have anticipated and guarded against.

41. Defendant was also on notice that the federal government has been concerned about data security. In 2020, during a SPARK Cybersecurity Virtual Event, Tim Hauser, deputy assistant secretary for national office operations at the US Department of Labor's Employee Benefits Security Administration observed that retirement plan administrators were being targeted for their wealth of personal, private financial information. The warning stated that:

> When a plan fiduciary is hiring somebody who is going to be responsible for confidential, personal information, or who's going to be running systems to keep track of people's account balances and the like, there's a responsibility to make sure that you've hired that person prudently, that firm prudently…And if you think about plans and the universe I described, that's just shy of $11 trillion, and with personal health and pension data, there are a lot of tempting targets there and what we've seen in our own enforcement actions, especially in our criminal programs, vulnerabilities are taken advantage of.[4]

42. The Department of Labor ("DOL") has also warned retirement plan administrators about the importance of protecting their customers' confidential information, noting that the "DOL's No. 1 concern is whether the firm is meeting current standards and addressing vulnerabilities, particularly as they change and evolve. 'If we were in looking at a recordkeeper or a TPA for cybersecurity, we'd want to see that there's a formal well-documented cybersecurity

[4] Ted Godbout, *DOL to Issue Guidance, Ramp up Investigations on Cybersecurity*, NAT'L ASS'N OF PLAN ADVISORS (Oct. 29, 2020), https://www.napa-net.org/news-info/daily-news/dol-issue-guidance-ramp-investigations-cybersecurity

program, that there are procedures, guidelines and standards in place, that they're regularly updated and that they're actually implemented'"[5]

43. The number of US data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[6] In 2017, a new record high of 1,579 breaches were reported—representing a 44.7 percent increase.[7] That trend continues.

44. The average time to identify and contain a data breach is 287 days,[8] with some breaches going unrecognized for months leading to costly recover efforts and financial impact. Additionally, the median cost per US consumer incurred on each fraud-related data breach incident in 2020 was $450.[9] Data breaches and identity theft have a crippling effect on individuals and detrimental impact on the economy as a whole.[10]

45. A 2021 study conducted by Verizon showed that internal mismanagement of data security, including mis-delivery of emails, represents nearly 44 percent of the data breaches in the financial sector.[11] The majority of these incidents involve the sending or releasing of information to unauthorized actors.[12]

46. PII related data breaches continued to rapidly into 2021 when Transamerica was breached.[13]

---

[5] *Id.*
[6] Identity Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), https://www.idtheftcenter.org/surveys-studys.
[7] Identity Theft Resource Center, *2017 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/2017-data-breaches/.
[8] IBM SECURITY, COST OF A DATA BREACH REPORT 6 (2021) [hereinafter COST OF A DATA BREACH REPORT]
[9] Insurance Information Institute, *Facts + Statistics: Identity Theft and Cybercrime* (2020), https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#top
[10] *Id.*
[11] *Financial and Insurance Data Breaches*, VERIZON 2021 DIBR DATA BREACH SURVEY (2021), https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/financial-services-data-breaches/.
[12] *Id.*
[13] *2019 HIMSS Cybersecurity Survey*, https://www.himss.org/2019-himsscybersecurity-survey.

47. Almost half of the data breaches globally are caused by internal errors, either human mismanagement of sensitive information, or system errors.[14] Cybersecurity firm Proofpoint reports that since 2020, there has been an increase of internal threats through the misuse of security credentials or the negligent release of sensitive information.[15] To mitigate these threats, Proofpoint recommends that firms take the time to train their employees about the risks of such errors.[16]

48. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precaution for protection."[17]

49. To prevent and detect unauthorized access, including the systems changes that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

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

[14] COST OF A DATA BREACH REPORT, *supra* note 8, at 30.
[15] *The Human Factor 2021*, PROOFPOINT (July 27, 2021), https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-human-factor-report.pdf.
[16] *Id.*
[17] *See How to Protect Your Networks from RANSOMWARE*, FBI (2016) https ://www. fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

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

- Manage the use of privileged accounts based on the principle of least privilege; no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

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

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

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

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

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

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

50. To prevent and detect unauthorized access to their systems, including the unauthorized access that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks . . .

- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net) . . .

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it . . .

- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic . . .[18]

[18] *See Security Tip (ST19-001) Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (Apr. 11, 2019), https://us-cert.cisa.gov/ncas/tips/ST19-001.

51. To prevent and unauthorized access, including the access by other plan administrators that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**
  - Apply the latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privilege credentials;
- **Thoroughly investigate and remediate alerts**
  - Prioritize and treat commodity malware infections as potential full compromise

- **Include IT Pros in security discussions**
  - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

- **Build credential hygiene**
  - use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

- **Apply principle of least-privilege**
  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events

- **Harden infrastructure**
  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[19]

[19] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT (Mar. 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-apreventable-disaster/.

52. These are basic, common-sense email security measures that every business, not only those who handle sensitive financial information, should be doing. Transamerica, with its heightened standard of care should be doing even more. But by adequately taking these common-sense solutions, Transamerica could have prevented this Data Breach from occurring.

53. Charged with handling sensitive PII including financial information, Transamerica knew, or should have known, the importance of safeguarding its customers' Private Information that was entrusted to it and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Transamerica's patients as a result of a breach. Transamerica failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

54. With respect to training, Transamerica specifically failed to:

- Implement a variety of anti-ransomware training tools, in combination, such as computer-based training, classroom training, monthly newsletters, posters, login alerts, email alerts, and team-based discussions;
- Perform regular training at defined intervals such as bi-annual training and/or monthly security updates; and
- Craft and tailor different approaches to different employees based on their base knowledge about technology and cybersecurity.

55. The PII was also maintained on Transamerica's computer system in a condition vulnerable to cyberattacks such as through the infiltration of Defendant's negligently maintained systems. The mechanism of the unauthorized access and the potential for improper disclosure of Plaintiff's and class members' PII was a known risk to Transamerica, and thus Transamerica was on notice that failing to take reasonable steps necessary to secure the PII from those risks left the PII in a vulnerable position.

C. The Monetary Value of Privacy Protections and Private Information

56. The fact that Plaintiff's and class members' Private Information was stolen—and is likely presently offered for sale to cyber criminals—demonstrates the monetary value of the Private Information.

57. At all relevant times, Defendant was well aware that Private Information it collects from Plaintiff and class members is highly sensitive and of significant property value to those who would use it for wrongful purposes.

58. Private Information is a valuable property right that is an important commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft and financial fraud.[20] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII including sensitive financial information on multiple underground Internet websites, commonly referred to as the dark web.

59. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[21]

---

[20] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft .

21 *Public Workshop: The Information Marketplace: Merging and Exchanging Consumer Data*, FED. TRADE COMM'N Tr. at 8:2-8 (Mar. 13, 2001), https://www.ftc.gov/sites/default/files/documents/public_events/information-marketplace-merging-and-exchanging-consumer-data/transcript.pdf.

60. Commissioner Swindle's 2001 remarks are even more relevant today, as consumers' personal data functions as a "new form of currency" that supports a $26 Billion per year online advertising industry in the United States.[22]

61. The FTC has also recognized that consumer data is a new (and valuable) form of currency. In an FTC roundtable presentation, another former Commissioner, Pamela Jones Harbour, underscored this point:

> 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.[23]

62. Recognizing the high value that consumers place on their Private Information, many companies now offer consumers an opportunity to sell this information.[24] The idea is to give consumers more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, consumers will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

63. Consumers place a high value not only on their Private Information, but also on the privacy of that data. Researchers have begun to shed light on how much consumers value their

---

[22] *See* Julia Angwin & Emily Steel, *Web's Hot New Commodity: Privacy*, The Wall Street Journal (Feb. 28, 2011), http://online.wsj.com/article/SB10001424052748703529004576160764037920274.html [hereinafter *Web's New Hot Commodity*].

[23] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

24 *Web's Hot New Commodity*, *supra* note 17.

data privacy, and the amount is considerable. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[25]

64. The value of Plaintiff and class members' Private Information on the black market is substantial. Sensitive financial information can sell for as much as $1000.[26] This information is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's information.

65. The ramifications of Transamerica's failure to keep its customers' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to 12 months or even longer.

66. Approximately 21% of victims do not realize their identify has been compromised until more than two years after it has happened.[27] This gives thieves ample time to make fraudulent charges under the victim's name.

67. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information it maintains is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud. Defendant should have particularly been aware of these risks given the significant number of data breaches affecting the financial industry and related industries.

68. Had Defendant remedied the deficiencies in its security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would

25 *See* U.S. Dep't of Justice, *Victims of Identity Theft,* OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

[26] *See* Zachary Ignoffo, *Dark Web Price Index 2021*, PRIVACY AFFAIRS (Nov. 21, 2021), https://www.privacyaffairs.com/dark-web-price-index-2021/

[27] *See Medical ID Theft Checklist,* IDENTITYFORCE https://www.identityforce.com/blog/medical-id-theft-checklist-2.

have prevented the ransomware attack into their systems and, ultimately, the theft of their customers' Private Information.

69. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about, or related to, an individual for which there is a possibility of logical association with other information is of great value to hackers and thieves. Indeed, "there is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer or device even if the individual pieces of data do not constitute PII."[28] For example, different PII elements from various sources may be able to be linked in order to identify an individual, or access additional information about or relating to the individual.[29] Based upon information and belief, the unauthorized parties utilized the Private Information they obtained through the Data Breach to obtain additional information from Plaintiff and class members that was misused.

70. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

71. Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts. Thus, even if payment card information were not involved in the

[28] *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report*, FED. TRADE COMM'N 35-38 (Dec. 2010), https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework.

[29] *See id.* (evaluating privacy framework for entities collecting or using consumer data with can be "reasonably linked to a specific consumer, computer, or other device").

Data Breach, the unauthorized parties could use Plaintiff's and class members' Private Information to access accounts, including, but not limited to email accounts and financial accounts, to engage in the fraudulent activity identified by Plaintiff.

72. Given these facts, any company that transacts business with customers and then compromises the privacy of customers' Private Information has thus deprived customers of the full monetary value of their transaction with the company.

73. Acknowledging the damage to Plaintiff and class members, Defendant instructed customers like Plaintiff to "remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft." Plaintiff and the other class members now face a greater risk of identity theft.

74. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breaches can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names. Plaintiff and class members have a property interest in their information and were deprived of this property when it was released to unauthorized actors through the negligent maintenance of Defendant's systems.

D. Transamerica Failed to Comply with FTC Guidelines

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

76. The FTC has promulgated numerous guides for businesses that 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.[30]

77. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cybersecurity guidelines for businesses.[31] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

78. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private 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.[32]

79. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15

[30] *Start With Security: A Guide for Business*, FED. TRADE. COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter *Start with Security*].
[31] *Protecting Personal Information: A Guide for Business*, FED. TRADE. COMM'M (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf- 0136_proteting-personal-information.pdf.
[32] *Start With Security: A Guide for Business*, FED. TRADE. COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [hereinafter Start with Security].

U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

80. Transamerica was at all times fully aware of its obligation to protect the Private Information of patients because of its position as a trusted retirement account administrator. Transamerica was also aware of the significant repercussions that would result from its failure to do so.

E. Damages to Plaintiff and the Class

81. Plaintiff and the Class have been damaged by the compromise of their Private Information in the Data Breach.

82. The ramifications of Transamerica's failure to keep patients' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to the victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[33]

83. In addition to its obligations under state laws and regulations, Defendant owed a common law duty to Plaintiff and class members to protect Private Information entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

84. Defendant further owed and breached its duty to Plaintiffs and class members to implement processes and specifications that would detect a breach of its security systems in a

[33] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

85. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise cause the identity theft and misuse to Plaintiff's and class members' Private Information as detailed above, and Plaintiffs are now at a heightened and increased risk of identity theft and fraud.

86. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

87. Some of the risks associated with the loss of personal information have already manifested themselves in Plaintiff Giannini's case. Mr. Giannini received a cryptically written notice letter from Defendant stating that his information was released, and that he should remain vigilant of fraudulent activity on his accounts, with no other explanation of where this information could have gone, or who might have access to it. Mr. Giannini has already spent hours on the phone trying to determine what negative effects may occur from the loss of his personal information.

88. In addition to spending time on the phone monitoring his credit accounts, Plaintiff Giannini has also received an influx of spam calls and emails. In addition to these issues, he has

received notices of purchase requests and applications for services in his name that he has never asked for or ordered, directly affecting his credit and financial record.

89. In just one example of these fraudulent charges made without Mr. Giannini's consent after the Data Breach occurred in or around June of 2021, he received a bill in his name related to cellular data equipment that he never ordered. The information needed to place such a fraudulent purchase order, including Mr. Giannini's name, social security number, address, and phone number, was accessible to the unauthorized parties in the Data Breach incident and would have allowed this misuse or sale of his information to malicious actors who instigated such fraudulent charges.

90. Plaintiff and the Class have suffered or face a substantial risk of suffering out-of-pocket losses such as fraudulent charges on online accounts, credit card fraud, loans opened in their names, and similar identity theft.

91. Plaintiff and class members have, may have, and/or will have incurred out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

92. Plaintiff and class members did not receive the full benefit of the bargain, and instead received services that were of a diminished value to that described in their agreements with Transamerica. They were damaged in an amount at least equal to the difference in the value of the services with data security protection they paid for and the services they received.

93. Plaintiff and class members would not have obtained services from Defendant had Defendant told them that it failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from theft.

94. Plaintiff and the Class will continue to spend significant amounts of time to monitor their financial accounts for misuse.

95. The theft of Social Security Numbers, which were purloined as part of the Data Breach, is particularly detrimental to victims. The U.S. Social Security Administration ("SSA") warns that "[i]dentity theft is one of the fastest growing crimes in America."[34] The SSA has stated that "[i]dentity 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."[35] In short, "[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems."[36]

96. In fact, a new Social Security number is substantially less effective where "other personal information, such as [the victim's] name and address, remains the same" and for some victims, "a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit."[37]

97. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. Private Information can be used to submit false insurance claims. As a result, Plaintiff and class members now face a real and continuing immediate risk of identity theft and other

34 *Identity Theft And Your Social Security Number*, SOCIAL SECURITY ADMIN. (Dec. 2013), http://www.ssa.gov/pubs/EN-05-10064.pdf.
35 *Id.*
36 *Id.*
37 *Id.*

problems associated with the disclosure of their Social Security numbers, and will need to monitor their credit for an indefinite duration. For Plaintiff and class members, this risk creates unending feelings of fear and annoyance. Private information is especially valuable to identity thieves. Defendant knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

98. As a result of the Data Breach, Plaintiff and class members' Private Information has diminished in value.

99. The Private Information belonging to Plaintiff and class members is private, private in nature, and was left inadequately protected by Defendant who did not obtain Plaintiff or class members' consent to disclose such Private Information to any other person as required by applicable law and industry standards. Defendant disclosed information about Plaintiff and the class that was of an extremely personal, sensitive nature as a direct result of its inadequate security measures.

100. The Data Breach was a direct and proximate result of Defendant's failure to (a) properly safeguard and protect Plaintiff's and class members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and class members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

101. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect customer data.

102. Defendant did not properly train their employees to identify and avoid unauthorized access to the network.

103. Had Defendant remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiff and class members' Private Information.

104. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

105. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[38]

106. Other than offering 24months of credit monitoring, Defendant did not take any measures to assist Plaintiff and class members other than telling them to simply do the following:

- remain vigilant for incidents of fraud and identity theft;
- review account statements and monitor credit reports for unauthorized activity;
- obtain a copy of free credit reports;
- contact the FTC and/or the state Attorney General's office;

[38] *See* U.S. Dep't of Justice, *Victims of Identity Theft*, OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

- enact a security freeze on credit files; and
- create a fraud alert.

None of these recommendations, however, require Defendant to expend any effort to protect Plaintiff and class members' Private Information.

107. Defendant's failure to adequately protect Plaintiff and class members' Private Information has resulted in Plaintiff and class members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money–while Defendant sits by and does nothing to assist those affected by the incident. Instead, as Transamerica's Data Breach Notice indicates, it is putting the burden on Plaintiff and class members to discover possible fraudulent activity and identity theft.

108. While Defendant offered two years of credit monitoring, Plaintiff could not trust a company that had already breached his data. The credit monitoring offered from Equifax does not guarantee privacy or data security for Plaintiff, who would have to expose his information once more to get monitoring services. Thus, to mitigate harm, Plaintiff and class members are now burdened with indefinite monitoring and vigilance of their accounts.

109. Moreover, the offer of 24 months of identity monitoring to Plaintiffs and Class Members is woefully inadequate. While some harm has already begun, the worst may be yet to come. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is acquired and when it is used. Furthermore, identity monitoring only alerts someone to the fact that they have already been the victim of identity theft (i.e., fraudulent acquisition and use of another person's Private Information) – it does not prevent

identity theft.[39] This is especially true for many kinds of financial identity theft, for which most credit monitoring plans provide little or no monitoring or protection.

110. Plaintiff and class members have been damaged in several other ways as well. Plaintiff and class members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their Private Information. Plaintiff and class members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming activity. Plaintiff and class members have also purchased credit monitoring and other identity protection services, purchased credit reports, placed credit freezes and fraud alerts on their credit reports, and spent time investigating and disputing fraudulent or suspicious activity on their accounts. Plaintiff and class members also suffered a loss of the inherent value of their Private Information.

111. The Private Information stolen in the Data Breach can be misused on its own, or can be combined with personal information from other sources such as publicly available information, social media, etc. to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen Private Information to send spear-phishing emails to class members to trick them into revealing sensitive information. Lulled by a false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the individual agrees to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

[39] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-beworth-the-cost.html.

112. As a result of Defendant's failures to prevent the Data Breach, Plaintiff and class members have suffered, will suffer, and are at increased risk of suffering:

- The compromise, publication, theft and/or unauthorized use of their Private Information;
- Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from 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 and fraud;
- The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Private Information in its possession;
- Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and class members; and
- Anxiety and distress resulting fear of misuse of their Private Information.

113. In addition to a remedy for the economic harm, Plaintiff and class members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

114. Plaintiff incorporates by reference all other paragraphs of this Complaint as if fully set forth herein.

115. Plaintiff brings this action individually and on behalf of all other persons similarly situated (the "Class") pursuant to Federal Rule of Civil Procedure 23.

116. Plaintiff proposes the following Class definition subject to amendment based on information obtained through discovery. Notwithstanding, at this time, Plaintiff brings this action and seeks certification of the following Class:

> All persons nationwide whose Private Information was compromised as a result of the Data Breach discovered on or about June 2021 and who were sent notice of the Data Breach.

Excluded from the Class are Defendant and Defendant's affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

117. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

118. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all class members would be impracticable. On information and belief, the Nationwide Class numbers in the thousands.

119. **Commonality and Predominance—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

- Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;
- Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;
- Whether Defendant properly implemented its purported security measures to protect Plaintiff's and the Class's Private

Information from unauthorized capture, dissemination, and misuse;

- Whether Defendant took reasonable measures to determine the extent of the Data Breach after it first learned of same;
- Whether Defendant disclosed Plaintiff's and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;
- Whether Defendant willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiff's and the Class's Private Information;
- Whether Defendant was negligent in failing to properly secure and protect Plaintiff's and the Class's Private Information;
- Whether Defendant was unjustly enriched by its actions; and
- Whether Plaintiff and the other members of the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

120. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff, on behalf of herself and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

121. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiff's claims are typical of the claims of the other members of the Class because, among other things, all class members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiff.

122. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiff is an adequate representative of the Nationwide Class because their interests do not conflict with the interests of the Classes they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and Plaintiff will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and their counsel.

123. **Injunctive Relief—Federal Rule of Civil Procedure 23(b)(2).** Defendant has acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

124. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other members of the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant's wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and All class members)

125. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

126. Upon Defendant's accepting and storing the Private Information of Plaintiff and the Class in their computer systems and on their networks, Defendant undertook and owed a duty to Plaintiff and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendant knew that the Private Information was private and confidential and should be protected as private and confidential.

127. Defendant owed a duty of care not to subject Plaintiff's and the Class's Private Information to an unreasonable risk of exposure and theft because Plaintiff and the Class were foreseeable and probable victims of any inadequate security practices.

128. Defendant owed numerous duties to Plaintiff and the Class, including the following:

- to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting Private Information in their possession;
- to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and
- to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

129. Defendant also breached its duty to Plaintiff and class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to

unsecured Private Information. Furthering their dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiff's and class members' Private Information and potentially misuse the Private Information and intentionally disclose it to others without consent.

130. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches.

131. Defendant knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiff's and class members' Private Information.

132. Defendant breached their duties to Plaintiff and class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff and class members' Private Information.

133. Because Defendant knew that a breach of their systems would damage thousands of their customers, including Plaintiff and class members, Defendant had a duty to adequately protect their data systems and the Private Information contained thereon.

134. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers, which is recognized by laws and regulations including but not limited to common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to class members from a data breach.

135. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . .

practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

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

137. Defendant's own conduct also created a foreseeable risk of harm to Plaintiff and class members and their Private Information. Defendant's misconduct included failing to: (1) secure Plaintiff's and Class member's Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

138. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect class members' Private Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- Failing to adopt, implement, and maintain adequate security measures to safeguard class members' Private Information;
- Failing to adequately monitor the security of Defendant's networks and systems;
- Allowing unauthorized access to class members' Private Information;
- Failing to detect in a timely manner that class members' Private Information had been compromised; and
- Failing to timely notify class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages

139. Through Defendant's acts and omissions described in this Complaint, including its failure to provide adequate security and failure to protect Plaintiff's and class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and class members' Private Information during the time it was within Defendant's possession or control.

140. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to failing to adequately protect the Private Information and failing to provide Plaintiff and class members with timely notice that their sensitive Private Information had been compromised.

141. Neither Plaintiff nor the other class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

142. As a direct and proximate cause of Defendant's conduct, Plaintiff and class members suffered damages as alleged above.

143. Plaintiff and class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all class members.

COUNT II
Breach of Contract
(On Behalf of Plaintiff and All class members)

144. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

145. Plaintiff and other class members entered into valid and enforceable express contracts with Defendant under which Plaintiffs and other class members agreed to provide their Private Information to Defendant, and Defendant agreed to provide financial services and, impliedly, if not explicitly, agreed to protect Plaintiff and class members' Private Information.

146. To the extent Defendant's obligation to protect Plaintiffs' and other Class Members' Private Information was not explicit in those express contracts, the express contracts included implied terms requiring Defendant to implement data security adequate to safeguard and protect the confidentiality of Plaintiffs' and other class members' Private Information, including in accordance with trade regulations; federal, state and local laws; and industry standards. No Plaintiff would have entered into these contracts with Defendant without understanding that Plaintiffs' and other class members' Private Information would be safeguarded and protected; stated otherwise, data security was an essential implied term of the parties' express contracts.

147. A meeting of the minds occurred, as Plaintiff and other class members agreed, among other things, to provide their Private Information in exchange for Defendant's agreement to protect the confidentiality of that Private Information.

148. The protection of Plaintiff and class members' Private Information were material aspects of Plaintiff's and class members' contracts with Defendant.

149. Defendant's promises and representations described above relating to industry practices, and about Defendant' purported concern about their clients' privacy rights became terms of the contracts between Defendant and their clients, including Plaintiff and other class members. Defendant breached these promises by failing to comply with reasonable industry practices.

150. Plaintiff and class members read, reviewed, and/or relied on statements made by or provided by Transamerica and/or otherwise understood that Transamerica would protect its patients' Private Information if that information were provided to Transamerica.

151. Plaintiff and class members fully performed their obligations under the implied contract with Defendant; however, Defendant did not.

152. As a result of Defendant's breach of these terms, Plaintiffs and other class members have suffered a variety of damages including but not limited to: the lost value of their privacy; they did not get the benefit of their bargain with Defendant; they lost the difference in the value of the secure services Defendant promised and the insecure services received; the value of the lost time and effort required to mitigate the actual and potential impact of the Data Breach on their lives, including, inter alia, that required to place "freezes" and "alerts" with credit reporting agencies, to contact financial institutions, to close or modify financial accounts, to closely review and monitor credit reports and various accounts for unauthorized activity, and to file police reports; and Plaintiffs and other class members have been put at increased risk of future identity theft, fraud, and/or misuse of their Private Information, which may take years to manifest, discover, and detect.

153. Plaintiff and class members are therefore entitled to damages, including restitution and unjust enrichment, disgorgement, declaratory and injunctive relief, and attorney fees, costs, and expenses.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and All class members, in the Alternative to Count II)

154. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

155. Through their course of conduct, Defendant, Plaintiff, and class members entered into implied contracts for the provision of financial services, as well as implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and class members' Private Information.

156. Specifically, Plaintiff entered into a valid and enforceable implied contract with Defendant when he first entered into the financial services agreement with Defendant.

157. The valid and enforceable implied contracts to provide financial services that Plaintiff and class members entered into with Defendant include Defendant's promise to protect nonpublic Private Information given to Defendant or that Defendant creates on its own from disclosure.

158. When Plaintiff and class members provided their Private Information to Defendant in exchange for Defendant's services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

159. Defendant solicited and invited class members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and class members accepted Defendant's offers and provided their Private Information to Defendant.

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

161. Class members who paid money to Defendant reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

162. Under implied contracts, Defendant and/or its affiliated providers promised and were obligated to: (a) provide financial services to Plaintiff and class members; and (b) protect Plaintiff's and the class members' Private Information provided to obtain such benefits of such services. In exchange, Plaintiff and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

163. Both the provision of financial services and the protection of Plaintiff's and class members' Private Information were material aspects of these implied contracts.

164. The implied contracts for the provision of financial services—contracts that include the contractual obligations to maintain the privacy of Plaintiff's and class members' Private Information—are also acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Data Breach notification letter.

165. Defendant's express representations, including, but not limited to the express representations found in its Privacy Notice, memorializes and embodies the implied contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and protect the privacy of Plaintiff's and class members Private Information.

166. Consumers of financial services value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining such services. Plaintiff and class members would not have entrusted their Private Information to Defendant and entered into these implied contracts with Defendant without an understanding that their Private Information would be safeguarded and protected or entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

167. A meeting of the minds occurred, as Plaintiff and class members agreed and provided their Private Information to Defendant and/or its affiliated companies, and paid for the provided services in exchange for, amongst other things, both the provision of financial services and the protection of their Private Information.

168. Plaintiff and class members performed their obligations under the contract when they paid for Defendant's services and provided their Private Information.

169. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when the information was accessed and exfiltrated by the Data Breach.

170. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant Notice of Privacy Practices. Defendant did not maintain the privacy of Plaintiff's and class members Private Information as evidenced by its notifications of the Data Breach to Plaintiff and class members. Specifically, Defendant did not comply with industry standards, standards of conduct embodied in statutes like Section 5 of the FTCA, or otherwise protect Plaintiff's and class members private information as set forth above.

171. The Data Breach was a reasonably foreseeable consequence of Defendant's action in breach of these contracts.

172. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiff and class members did not receive full benefit of the bargain, and instead received financial and other services that were of a diminished value to that described in the contracts. Plaintiff and class members therefore were damaged in an amount at least equal to the difference in the value of the retirement accounts with data security protection they paid for and the services they received.

173. Had Defendant disclosed that its security was inadequate or that it did not adhere to industry-standard security measures, neither the Plaintiff, class members, nor any reasonable person would have utilized services from Defendant and/or its affiliated entities.

174. As a direct and proximate result of the Data Breach, Plaintiff and class members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

175. Plaintiff and class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

176. Plaintiff and class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all class members.

COUNT IV
Unjust Enrichment/Quasi-Contract
(On Behalf of Plaintiff and All class members)

177. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

178. Plaintiff and Class members conferred a monetary benefit on Defendant. Specifically, they purchased goods and services from Defendant and provided Defendant with their Private Information. In exchange, Plaintiff and Class members should have received from

Defendant the goods and services that were the subject of the transaction and should have been entitled to have Defendant protect their Private Information with adequate data security.

179. Defendant knew that Plaintiffs and Class members conferred a benefit on them and accepted or retained that benefit. Defendant profited from Plaintiffs' purchases and used Plaintiff's and Class member's Private Information for business purposes.

180. Defendant failed to secure Plaintiff and Class members' Private Information and, therefore, did not provide full compensation for the benefit the Plaintiff and Class members' Private Information provided.

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

182. If Plaintiffs and Class members knew that Defendant would not secure their Private Information using adequate security, they would not have used Defendant's services.

183. Plaintiff and Class members have no adequate remedy at law.

184. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class members conferred on them.

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

COUNT V
Breach of Fiduciary Duty
(On Behalf of Plaintiff and All class members)

186. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

187. In providing their Private Information to Defendant, Plaintiff and class members justifiably placed a special confidence in Defendant to act in good faith and with due regard to interests of Plaintiff and class members to safeguard and keep confidential that Private Information.

188. Defendant accepted the special confidence Plaintiff and class members placed in it, as evidenced by its assertion that it is "committed to protecting the privacy of [Plaintiff's] personal information" as included in the Data Breach notification letter.

189. In light of the special relationship between Defendant and Plaintiff and class members, whereby Defendant became a guardian of Plaintiff's and class members Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its customers, including Plaintiff and class members for the safeguarding of Plaintiff and Class member's Private Information.

190. Defendant has a fiduciary duty to act for the benefit of Plaintiff and class members upon matters within the scope of its customer's relationship, in particular, to keep secure the Private Information of its customers.

191. Defendant breached its fiduciary duties to Plaintiff and class members by failing to protect the integrity of the systems containing Plaintiff's and Class member's Private Information.

192. Defendant breached its fiduciary duties to Plaintiff and class members by otherwise failing to safeguard Plaintiff's and class members' Private Information.

193. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and class members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Cyber-Attack and Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Cyber-Attack and Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

194. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V
Breach of Confidence
(On Behalf of Plaintiff and All class members)

195. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

196. At all times during Plaintiff and Class members' interactions with Defendant, Defendant was fully aware of the confidential, novel, and sensitive nature of Plaintiff's and the Class members' Private Information that Plaintiff and Class members provided to Defendant.

197. As alleged herein and above, Defendant's relationship with Plaintiff and Class members was governed by expectations that Plaintiff and Class members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

198. Plaintiffs and Class members provided their respective Private Information to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Private Information to be disseminated to any unauthorized parties.

199. Plaintiffs and Class members also provided their respective Private Information to Defendant with the explicit understanding that Defendant would take precautions to protect that Private Information from unauthorized disclosure, such as following basic principles of information security practices.

200. Defendant voluntarily received in confidence Plaintiff and Class members' Private Information with the understanding that the Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

201. Due to Defendant's failure to prevent, detect, and/or avoid the Security Breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiffs' and Class members' Private Information, Plaintiffs' and Class members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class members' confidence, and without their express permission.

202. But for Defendant's disclosure of Plaintiffs' and Class members' Private Information in violation of the parties' understanding of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Security Breach was the direct and legal cause of the theft of Plaintiffs' and Class members' Private Information, as well as the resulting damages.

203. The injury and harm Plaintiffs and Class members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class members' Private Information. Defendant knew or should have known their security systems were insufficient to protect the Private Information that is coveted by thieves worldwide. Defendant also failed to observe industry standard information security practices.

204. As a direct and proximate cause of Defendant's conduct, Plaintiffs and Class members suffered damages as alleged above.

COUNT VI
Bailment
(On Behalf of Plaintiff and All class members)

205. Plaintiff incorporates by reference all of the above paragraphs, as though fully set forth herein.

206. Plaintiff and Class members delivered and entrusted their Personal Information to Defendant for the sole purpose of receiving services from Defendant.

207. In delivering their Personal Information to Defendant, Plaintiff and Class members intended and understood that Defendant would adequately safeguard their personal and financial information.

208. Defendant accepted possession of Plaintiffs and Class members' Personal Information. By accepting possession, Defendant understood that Plaintiffs and Class members

expected Defendant to safeguard their personal and financial information adequately. Accordingly, a bailment was established for the mutual benefit of the parties.

209. During the bailment, Defendant owed a duty to Plaintiffs and Class members to exercise reasonable care, diligence, and prudence in protecting their Personal Information.

210. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and Class members' Personal Information, resulting in the unlawful and unauthorized access to and misuse of such information.

211. Defendants further breached their duty to safeguard Plaintiffs' and Class members' Personal Information by failing to notify them individually in a timely and accurate manner that their information had been breached and compromised.

212. As a direct and proximate result of Defendant's breach of duty, Plaintiffs and Class members suffered consequential damages that were reasonably foreseeable to Defendants, including but not limited to the damages set forth herein.

COUNT VII
VIOLATION OF THE CALIFORNIA CONSTITUTION'S RIGHT TO PRIVACY
(Cal. Const., art. I, § 1)
(On Behalf of Plaintiff and class members)

213. Plaintiff fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

214. The California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possession, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Const., art. I. § 1.

215. Plaintiff and the Class have a legally recognized and protected privacy interest in the personal and financial information provided to and obtained by Defendant, including but not limited to an interest in precluding the dissemination or misuse of this sensitive and confidential information and the misuse of this information for malicious purposes such as theft of funds.

216. Plaintiff and the Class reasonably expected Defendant would prevent the unauthorized viewing, use, manipulation, exfiltration, theft, and disclosure of their personal and financial information and the unauthorized use of their Private Information.

217. Defendant's conduct described herein resulted in a serious invasion of privacy of Plaintiff and the Class, as the release of Private Information could highly offend a reasonable individual.

218. As a direct consequence of the actions as identified above, Plaintiff and the Class members suffered harms and losses including but not limited to economic loss, the loss of control over use of their identity, harm to their constitutional right to privacy, lost time dedicated to the investigation and attempt to cure harm to their privacy, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal and financial information disclosed.

COUNT VIII
VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW ("UCL"),
Cal. Bus. Prof. Code § 17200, *et seq.*,
(On Behalf of Plaintiff and class members)

219. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

220. Defendant violated California's Unfair Competition Law ("UCL") Cal. Bus. Prof. Code § 17200, *et seq.*, by engaging in unlawful, unfair or fraudulent business acts and practices

and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in the UCL, including, but not limited to, the following:

- By representing and advertising that it would maintain adequate data privacy and security practices and procedures to safeguard Plaintiff's and Class member's Personal and financial information from unauthorized disclosure, release, data breach, and theft; representing and advertising that Defendant would and did comply with the requirement of relevant federal and state laws relating to privacy and security of Plaintiff's and Class's Private Information; and omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Private Information;
- By soliciting and collecting Private Information from Plaintiff's and Class members without adequately protecting or storing Private Information;
- by violating the CMIA, Cal. Civ. Code § 56, *et seq*.

221. Defendant's practices were also contrary to legislatively declared and public policies that seek to protect consumer data and ensure that entities that solicit or are entrusted with personal data utilize appropriate security measures, as reflected by laws like the FTC Act, 15 U.S.C. § 45, and the CMIA, Cal. Civ. Code § 56, *et seq*.

222. As a direct and proximate result of Defendant's unfair and unlawful practices and acts, Plaintiff and the Class were injured and lost money or property, including but not limited to, overpayments Defendant received to maintain adequate security measures and did not, the loss of their legally protected interest in the confidentiality and privacy of their Personal and Financial Information, and additional losses described above.

223. Defendant knew or should have known that its computer systems were vulnerable and thus inadequate to safeguard Plaintiffs' and Class members' Private Information and that the

risk of a data breach or unauthorized access was highly likely. Defendant had resources to secure and/or prepare for protecting customer's Private Information in a Security Breach. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of the Class.

224. Plaintiff seeks relief under the UCL, including restitution to the Class of money or property that the Defendant may have acquired by means of Defendant's deceptive, unlawful, and unfair business practices, declaratory relief, attorney fees, costs and expenses (pursuant to Cal. Code Civ. P. § 1021.5), and injunctive or other equitable relief.

COUNT IX
VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT ("CRA"),
Cal. Bus. Prof. Code § 17200, *et seq.*,
(On Behalf of all Plaintiff and class members)

225. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

226. At all relevant times, Defendant was a "business" under the terms of the CRA as a retirement plan administrator operating in the State of California that owned or licensed computerized data that included the personal information of Plaintiff and the Class.

227. At all relevant times, Plaintiff and the Class were "customers" under the terms of the CRA as natural persons who provided personal information to Defendant for the purpose of purchasing or leasing a product or obtaining a service from Defendant.

228. Section 1798.82 requires disclosure "shall be made in the most expedient time possible and without unreasonable delay…." By the acts described above, Defendant violated the CRA by allowing unauthorized access to customers' personal and financial information and then failing to inform them when the unauthorized use occurred for weeks, thereby failing in

their duty to inform their customers of unauthorized access expeditiously and without unreasonable delay.

229. The Data Breach described herein is a "breach of the security system" under Section 1798.82.

230. As a direct consequence of the actions as identified above, Plaintiff and the Class incurred additional losses and suffered further harm to their privacy, including but not limited to economic loss, the loss of control over the use of their identity, harm to their constitutional right to privacy, lost time dedicated to the investigation of and attempt to recover the loss of funds and/or cure harm to their privacy, the need for future expenses and time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal and financial information disclosed, that they would have not otherwise lost had Defendant immediately informed them of the unauthorized use.

231. Plaintiff accordingly requests the Court enter an injunction requiring Defendant to implement and maintain reasonable security procedures, including, but not limited to: (1) order Defendant utilizes stronger industry standard data security measures and file transfer software for the transfer and storage of customer data; (2) order Defendants engage third party security auditors and/or penetration testers on a regular basis as well as internal security to conduct testing inclusive of simulated attacks and institution-wide personnel training; (3) order Defendants, consistent with industry standard practices, to periodically conduct internal training and education to inform internal personnel how to identify and contain a breach when it occurs, and how to respond to a breach; and (4) order Defendants to meaningfully educate its customers about threats they face as a result of losing their Private Information to unauthorized third parties.

232. Plaintiff further requests the Court require Defendant to identify all of its impacted clients, to what degree their information was stolen, and to notify all members of the Class who have not yet been informed of the Data Breach by written email within 24 hours of discovery of a breach, possible breach, and by mail within 72 hours.

233. As a result of Defendant's violations, Plaintiff and the Class are entitled to all actual and compensatory damages according to proof, to non-economic injunctive relief allowable under the CRA, and to such other and further relief as this Court may deem just and proper.

COUNT X
Violation of New York General Business Law § 349
N.Y. Gen. Bus. Law § 349 *et seq* (2019).
(On Behalf of Plaintiff and class members)

234. Plaintiff fully incorporates by reference all of the above paragraphs, as though fully set forth herein.

235. New York General Business Law ("NYGBL") § 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.

236. By reason of the conduct alleged herein, Defendant engaged in unlawful practices within the meaning of the NYGBL § 349. The conduct alleged herein is a "business practice" within the meaning of the NYGBL § 349, and the deception occurred within New York State.

237. Defendant stored Plaintiffs' and the Class members' Private Information in Defendant's electronic databases. Defendant knew or should have known they did not employ reasonable, industry standard, and appropriate security measures that complied with all relevant regulations and would have kept Plaintiffs' and the Class members' Private Information secure

and prevented the loss or misuse of Plaintiffs' and the Class members' Private Information. Defendant did not disclose to Plaintiffs and the Class members that their data systems were not secure.

238. Plaintiff, class members and Defendant each qualify as a party engaging in consumer transactions, as defined in N.Y. Gen. Bus. Law § 349(a).

239. Plaintiff and the Class never would have provided their sensitive and personal Private Information if they had been told or knew that Defendant failed to maintain sufficient security to keep such Private Information from being hacked and taken by others, and that Defendant failed to maintain the information in encrypted form.

240. Defendant violated the NYGBL §349 by misrepresenting, both by affirmative conduct and by omission, the safety of Defendant's many systems and services, specifically the security thereof, and their ability to safely store Plaintiffs' and the Class members' Private Information.

241. As alleged herein in this Complaint, Defendant 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 its services were of a particular standard or quality that it knew or should have known were of another;
- Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff 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 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 Cyber-Attack and data breach;

- Misrepresenting that it 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 it did not reasonably or adequately secure Plaintiff's and Class members' Private Information; and

  Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of 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 Security breach.

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

243. Such acts by Defendant 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 Defendant. 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, NYGBL § 349.

244. In addition, Defendants' failure to secure patients' PII violated the FTCA and there violates N.Y. Gen. Bus. Law § 349.

245. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the PII of Plaintiff and Class Members, deter hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

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

247. Defendant's violations of N.Y. Gen. Bus. Law § 349 has an impact and general importance to the public, including the people of New York. Thousands of New Yorkers have had financial accounts maintained by Transamerica, many of whom have been impacted by the Data Breach. In addition, New York residents have a strong interest in regulating the conduct of its retirement and investment services administrators, whose polices described herein have affected thousands of people across the country.

248. 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 attorney's fees), and such other relief as the Court deems just and proper.

249. On information and belief, Transamerica formulated and conceived of the systems it used to compile and maintain patient information largely within the state of New York, 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.

250. Most, if not all, of the alleged misrepresentations and omissions by Transamerica that led to inadequate safety measures to protect patient information occurred within or were approved within Indiana.

251. Defendant's implied and express representations that they 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 data security services were of another, inferior quality), in violation of N.Y. Gen. Bus. Law § 349.

252. Accordingly, Plaintiff, on behalf of himself and class members, bring 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 XI
Violations of New York Information Security Breach and Notification Act
N.Y. Gen. Bus. Law § 899-aa
(On Behalf of all Plaintiffs and All Class Members)

253. Plaintiff fully incorporates all of the above paragraphs, as though fully set forth herein.

254. The acts and practices alleged herein occurred in trade or commerce in the state of New York.

255. The Breach, which compromised the Private Information, including the Social Security numbers, of New York citizens constitutes a "breach of security," as that term is defined by NY Gen. Stat.§ 899-aa.

256. In the manner described herein, the defendants unreasonably delayed the disclosure of the breach of security of personal information within the meaning of NY. Gen. Stat. § 899-aa.

257. Pursuant to NY. Gen. Stat. § 89-9aa the Defendants' failure to disclose the breach following the discovery to each New York resident whose personal information was, or was reasonably believed to have been, accessed by an unauthorized person through the breach constitutes an unfair trade practice pursuant to NY. Gen. Stat. § 899-aa.

DEMAND FOR JURY TRIAL

Plaintiffs demands a trial by jury of all claims so triable.

REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

a. For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Classes;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and class members' Private Information, and from failing to issue prompt, complete and accurate disclosures to Plaintiff and class members;

c. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e. Ordering Defendant to pay for not less than three (3) years of credit monitoring services for Plaintiff and the Classes;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of punitive damages, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded; and such other and further relief as this court may deem just and proper.

Date: December 2, 2021

Respectfully submitted,

/s/ Nicholas A. Migliaccio

Nicholas A. Migliaccio (New York Bar No. 4035838)
nmigliaccio@classlawdc.com
Jason S. Rathod (pro hac vice anticipated)
jrathod@classlawdc.com
Migliaccio & Rathod LLP
412 H Street NE
Washington, DC 20002
Tel: (202) 470-3520
Fax: (202) 800-2730

Counsel for Plaintiff