IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

Simeon Taylor, Plaintiff, vs. Allianz Life Insurance Company of North America, Defendant.	Case No: 0:25-cv-3020 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

INTRODUCTION

Plaintiff individually and on behalf of all others similarly situated, upon personal knowledge of facts and information and belief, pertaining to himself against Defendant Allianz Life Insurance Company of North America ("Allianz Life" or "Defendant"), and in support thereof alleges as follows:

NATURE OF THE ACTION

1. Plaintiff is among the roughly 1.4 million individuals in the United States who had their sensitive, personally identifiable information ("PII") and protected health information ("PHI" and together with PII, "Personal Information") stolen from a database operated by Defendant.

2. Starting on or around July 16, 2025, hackers successfully exploited a vulnerability in a CRM system[1] that Defendant used to store data of customers, financial

[1] "CRM system" refers to a Customer Relationship Management system, which acts as a central hub for storing data and can integrate with other business systems like email, social media, and e-commerce platforms.

professionals, and employees. This breach exposed over one million individuals' Personal Information, including financial and medical data (the "Data Breach").

3. Defendant's parent, Allianz SE ("Allianz"), has acknowledged the real risk of a data breach for years:

- 2015: Allianz warns that "cyber risk is the risk most underestimated by businesses" and that "everyone is a target".[2]
- 2020: "In addition to being the top risk globally, Cyber incidents is among the top three risks in many of the countries surveyed; in Austria, Belgium, France, India, South Africa, South Korea, Spain, Sweden, Switzerland, the UK and the US it also ranks as the top business risk."[3]
- 2023: "Cyber incidents is the number one business risk for companies around the world, according to the Allianz Risk Barometer 2023, with data breaches the cyber exposure of most concern."[4]

4. This year, Allianz further admitted the critical threat of cyber attacks is still the top risk for companies: "Cyber incidents such as ransomware attacks, data breaches,

[2] Allianz, *A guide to cyber risk* (Sept. 2015) (https://commercial.allianz.com/news-and-insights/reports/a-guide-to-cyber-risk.html).

[3] Allianz, Press Release, *Allianz Risk Barometer 2020: Cyber top peril for companies globally for the first time* (https://www.allianz.com/content/dam/onemarketing/azcom/Allianz_com/press/document/Allianz-Risk-Barometer-2020-press-release_EN.pdf).

[4] Allianz, *Cyber: dealing with a data breach* (April 2023) (https://commercial.allianz.com/news-and-insights/expert-risk-articles/cyber-data-breach.html).

and IT disruptions, rank as the top global risk in the Allianz Risk Barometer—and by a higher margin than ever before."[5]

5. Despite this knowledge, Defendant gathered and collected this vast volume of Personal Information through their business operations and did not adequately protect this data. As an insurance company that provides a comprehensive range of insurance products and services to its clients, it obtained access to the data involved in millions of insurance contracts and claims, allowing it to aggregate substantial amounts of medical records and histories, financial records, and other sensitive information of thousands of individuals.

6. While Defendant held the Personal Information of approximately 1.4 million Americans, they failed to use basic data security measures necessary to protect it. This is despite Defendant promising:

> Allianz cares about your personal data. Our mission is to ensure the Allianz' privacy strategy and framework enable our businesses to maintain the trust of customers, employees and other stakeholders in our handling of personal data. We are committed to the highest standards of data protection and privacy compliance by handling personal data responsibly, transparently, with due care and in a fair and lawful manner. We use it only for specified and legitimate purposes and only keep it for as long as is needed. We never share it with anyone who is not authorized to access it.
>
> We strive to communicate honestly and openly about actions that involve the personal data we process. We integrate data protection into the design of our products (privacy by design) and take appropriate steps to protect personal data and keep it secure
>
> On this page, we would like to introduce you to our Privacy framework and activities.

[5] Allianz, *Allianz Risk Barometer 2025* (Jan. 2025) (https://commercial.allianz.com/news-and-insights/expert-risk-articles/allianz-risk-barometer-2025-cyber-incidents.html).

7. Beginning as early as July 16, 2025, hackers compromised Defendant's database and gained access to its systems.[6] Although many details of the Data Breach have not been publicly released, the nature of the breach illustrates Defendant's severe security deficiencies.

8. Allianz has instructed companies on how to take steps to protect against cyber attacks that its own subsidiary, Defendant, turned a blind eye to. Indeed, Allianz has stated that the breach was due to "social engineering technique" that often involves a scheme to gain access. Even though Allianz has stressed (at least as early as 2015) the ten steps a company should take to protect itself, Defendant did not sufficiently secure its own system and/or ensure that any CRM system was properly vetted for cybersecurity.[7]

[6]Larence Abrams, *Allianz Life confirms data breach impacts majority of 1.4 million customers*, Bleeping Computer (https://www.bleepingcomputer.com/news/security/allianz-life-confirms-data-breach-impacts-majority-of-14-million-customers/).

[7]Allianz Global Corporate & Specialty, *A Guide to Cyber Risk* (https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/AGCS-Cyberrisk-report.pdf).

10 steps to cyber security

STEP 1 Implement an effective governance structure, maintain board engagement and produce appropriate information security policies which should include:

STEP 2 User education and awareness training

STEP 3 Monitoring policies and procedures for all networks and systems

STEP 4 Incident management procedures, including response and disaster recovery

STEP 5 Network security policies and procedures

STEP 6 Management and control of user privileges

STEP 7 Secure configuration guidance

STEP 8 Malware protection procedures

STEP 9 Control of removable media usage

STEP 10 Monitoring of mobile and home working procedures

9. Defendant has yet to provide information about the CRM system connected to the hack, but sources suspect that the attack can be attributed to the ShinyHunters threat group—hackers known to be targeting Salesforce CRM customers in social engineering attacks.[8]

10. The hackers are reported to be employing tactics including impersonating IT support staff and requesting that employees accept a connection to Salesforce Data Loader.

[8] Emma Woollacott, *Everything we know about the Allianz Life data breach so far*, IT PRO (July 28, 2025) (https://www.itpro.com/security/data-breaches/everything-we-know-about-the-allianz-life-data-breach-so-far).

Once this connection is made, the hackers are exfiltrating data from Salesforce.[9] In "around 80% of ransomware incidents losses could have been avoided if the organizations had followed best practices. Regular patching, multi-factor authentication, as well as information security and awareness training and incident response planning are essential to avoiding ransomware attacks and also constitute good cyber hygiene," according to Rishi Baviskar, Global Cyber Experts Leader at AGCS Risk Consulting. "If companies adhere to best practice recommendations there is a good chance that they will not become ransomware victims. Numerous security gaps can be closed, often with simple measures."[10]

11. Finally, although "clear communication is key" and consumers should receive "timely information" from things like regional and national press and social media, Defendant has done none of that as of July 27, 2025. Indeed, Defendant has not even provided notice of the breach that it will send out to those impacted.[11]

12. Had Defendant employed basic, long-established, and recommended security tools, the Data Breach should have been easily thwarted. However, Defendant did not employ best practices for data security.

13. Once in Defendant's network, the hackers successfully exfiltrated policyholders' Personal Information from Defendant's server. Despite its sensitivity, Defendant did not store the data sufficiently securely to prevent its theft.

---

[9] *Id.*
[10] Allianz Commercial, *Ransomware trends: Risks and Resilience* (Oct. 2021) (https://commercial.allianz.com/news-and-insights/reports/cyber-risk-trends-2021.html_).
[11] *Id.*

14. Both before and after the Data Breach, Defendant repeatedly put its interests above those of the impacted policyholders. However, Defendant owed duties to Plaintiff and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their Personal Information against unauthorized access and disclosure. Defendant breached those duties by, among other things, failing to implement and maintain reasonable security procedures and practices to protect the Personal Information entrusted to them from unauthorized access and disclosure.

15. As a result of Defendant's inadequate security and breach of its duties and obligations, the Data Breach occurred and Plaintiff's and Class Members' Personal Information was accessed by, and disclosed to, unauthorized third-party actors.

16. Plaintiff and Class Members have experienced extensive harms as a result, including, among other things: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (8) a continued substantial and imminent risk of the misuse of their Personal Information.

17. Upon information and belief, Defendant breached its duties and obligations by failing, in one or more of the following ways: (1) failing to design, implement monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to

design, implement, and maintain reasonable data retention policies; (3); failing to adequately train employees on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class Members of Defendant's inadequate security practices; (6) failing to encrypt or adequately encrypt the Private Information; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attach, and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

18. Defendant understood that, in order to receive services, Plaintiff and Class Members were required to entrust their highly sensitive Personal Information to Defendant. Plaintiff and Class Members entrusted this information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

19. This instant action seeks to hold Defendant accountable for their inadequate security and the resulting Data Breach. Plaintiff thus brings this Complaint on behalf of themselves and all similarly situated individuals whose Personal Information was stolen as a result of the Data Breach. Plaintiff, on behalf of themself and all other Class Members, brings the below common law tort claims and state statutory claims seeking declaratory and injunctive relief, monetary damages including punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

20. Plaintiff Simeon Taylor is a citizen of Texas, residing in Dallas, Texas. On or about July 16, 2025, Plaintiff's Personal Information was accessed and exfiltrated from Defendant's networks. Plaintiff Taylor estimates he spent about several hours responding to the Data Breach by researching the Data Breach, contacting his bank about fraudulent activity and getting new bank cards issued, monitoring her accounts for suspicious activity and fielding spam/phishing calls. Plaintiff Taylor continues to review his accounts for fraud. Prior to the Data Breach, Plaintiff Taylor does not recall experiencing any type of fraud in his banking and credit card history. Plaintiff Taylor is very careful about sharing his own Personal Information and has never knowingly transmitted unencrypted Personal Information over the internet or any other unsecured source. Plaintiff Taylor stores any and all documents containing Personal Information in a secure location and destroys any documents he receives in the mail that contain any Personal Information, or that may contain any information that could otherwise be used to compromise his identity and financial accounts. Moreover, Plaintiff Taylor diligently chooses unique usernames and passwords for his various online accounts.

21. Defendant Allianz Life Insurance Company of North America is a stock insurance corporation with its principal place of business located at 5701 Golden Hills Drive, Minneapolis, MN 55416.

JURISDICTION AND VENUE

22. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum

or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) there are Class Members who are diverse from Defendant, and (4) there are more than 100 Class Members.

23. This Court has personal jurisdiction over Defendant because at all relevant times, Defendant operated its principal places of business in this State and also because Defendant took actions in this State that gave rise to the Data Breach and, thus, to Plaintiff's and the Class's claims.

24. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a)(1) because Defendant's principal place of business is in this District and many of Defendant's acts complained of herein occurred within this District.

25. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because all claims alleged herein form part of the same case or controversy.

FACTUAL ALLEGATIONS

26. Defendant warrants to its clients that it is "a leading provider of annuities and life insurance", "dedicated to helping secure the future of [Defendant's] customers."[12] Defendant invites potential clients to "depend on [Defendant] for the long term" to "deliver dependable, long-term results," as Defendant has "extensive capabilities that allow [Defendant] to monitor and control risk in real time."[13]

[12] *Why Allianz* (https://www.allianzlife.com/why-allianz)
[13] *Id.*

27. Allianz Life is a subsidiary of Allianz SE, a global financial services group with more than 128 million customers and one of the largest companies, insurers, and asset managers in the world.[14]

28. Because insurance coverage requires would-be policyholders to provide their personal and financial history to the insurer, the data stored on Defendant's network includes not only full names, phone numbers, addresses, Social Security numbers, dates of birth, and email addresses, but also medical histories, specific treatment information, and insurance records.

29. Defendant has kept and maintained the Personal Information it has collected over years of providing its services from its policyholders, employees and other financial professionals, including aggregating and storing information in the server that would ultimately be accessed and exfiltrated by unauthorized users during the Data Breach.

30. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and Class Members.

31. Personal Inforamtionhas never been more ubiquitous or more valuable. The global investment banking firm RBC Capital Markets estimates that 30% of the world's data is now being generated in the healthcare sector and that healthcare data alone will grow at a Compound Annual Growth Rate ("CAGR") of 36% by 2025.[15] This development is the result of improved software technologies, increased detail in information collected

[14] *Id.*
[15] *The Claims Processing Manual,* 2019, AMERICAN MEDICAL BILLING ASSOCIATION, (https://www.ambastore.net/product_p/advancedclaimsmanual1.htm).

as part of medical encounters, more sophisticated billing processes, improved data storage, and rapid conversion to EHR. Between 2009 and 2019, U.S. hospital adoption of EHR systems grew from 6.6% to 81.2%. [16]

32. This accumulation of data creates the opportunity for commercial exploitation. Commercial data analytic efforts and techniques have evolved simultaneously to accommodate the volume, velocity and variety of these innumerable individual health records.[17] The global data analytics market was valued at $43.1 billion in 2023 and expected to grow by 23% the next year, reaching $53 billion in 2024.[18] The consulting firm McKinsey estimates healthcare data analytics profits are growing at a CAGR of 22%.[19] One healthcare data firm—IQVIA, a "global provider of advanced analytics, technology solutions, and clinical research services" —reported revenue of $14.9 billion for 2023.

33. According to its Privacy Notice, Defendant collects and stores Personal Information that specifically includes social security numbers and income, account balances and payment history, and transaction history and insurance claim history.[20]

---

[16] *Compare PPOs, EPOs, and HMOs*, CALIFORNIA DEPARTMENT OF INSURANCE, (https://www.insurance.ca.gov/01-consumers/110-health/10-basics/compare.cfm).
[17] *Types of Health Coverage*, CALIFORNIA DEPARTMENT OF INSURANCE, (https://www.insurance.ca.gov/01-consumers/110-health/10-basics/types.cfm).
[18] *Change Healthcare, Form 10-K for fiscal year ending March 31, 2022*, SEC, https://www.sec.gov/Archives/edgar/data/1756497/000175649722000007/chng-20220331x10k.htm.
[19] Henderson, Morgan A., and Morgane C. Mouslim, *Facts About Hospital-Insurer Contracting*, *The American Journal of Managed Care* 30, no. 2 (Feb. 2024).
[20] *Privacy Notice Allianz Life of North America*, (https://www.allianzlife.com/-/media/Files/Global/documents/2016/05/09/17/32/M40018.pdf)

34. By obtaining, collecting, and storing Plaintiff's and Class Members' Personal Information, Defendant assumed legal and equitable duties and knew that Defendant was responsible for protecting Plaintiff's Personal Information from unauthorized disclosure.

35. Defendant specifically indicates the purposes for which it obtains, collects, and stores Plaintiff's and Class Member's Personal Information, including for everyday business purposes and joint marketing with third parties. Plaintiff and Class Members have no way to limit this sharing of data.[21]

Reasons we can share your personal information	Does Allianz share?	Can you limit this sharing?
For our everyday business purposes – For example: to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
For our marketing purposes – to offer our products and services to you	Yes	No
For joint marketing with other financial companies	Yes	No
For our affiliates' everyday business purposes – information about your transactions and experiences	Yes	No

36. In the Privacy Notice, Defendant warrants: to "protect [] personal information from authorized access and use, we use security measures that comply with federal and state law," including using "security controls, including encryption, firewalls, [and] advanced malware detection".

37. Hence, prior to the Data Breach, Defendant recognized and acknowledged that its customers and those it services have placed their trust in Allianz Life to protect the confidentiality and privacy of their data. Defendant is and was responsible to all those who place their trust in it to maintain data security, including Plaintiff and Class Members.

[21] *Id*. at 1.

38. Defendant represented to the public that these are not mere words or policies. Allianz Life's President and CEO Jasmine Jirele has stated that "As a leading provider of innovative financial products to help manage risk, we are dedicated to helping secure the future of our customers."[22]

39. Given their prior and current representations and experience handling highly sensitive PII and PHI, Defendant understood the need and requirements to protect policyholders' Personal Information and prioritize data security.

A. The Breach

40. Defendant has yet to provide information about the CRM system connected to the hack, but sources suspect that the attack can be attributed to the ShinyHunters threat group—hackers known to be targeting Salesform CRM customers in social engineering attacks.[23]

41. Last month, Mandiant—a company offering cyber security services—warned that ShinyHunters had begun to target SalesForce CRM customers.[24]

42. The hackers are reported to be employing tactics including impersonating IT support staff and requesting that employees accept a connection to Salesforce Data Loader. Once this connection is made, the hackers are exfiltrating data from Salesforce.[25]

---

[22] *Why Allianz* (https://www.allianzlife.com/why-allianz).
[23] Emma Woollacott, *Everything we know about the Allianz Life data breach so far*, IT Pro (July 28, 2025) (https://www.itpro.com/security/data-breaches/everything-we-know-about-the-allianz-life-data-breach-so-far).
[24] Lawrence Abrams, *Allianz Life confirms data breach impacts majority it 1.4 million customers*, Bleeping Computer (July 26, 2025) (https://www.bleepingcomputer.com/news/security/allianz-life-confirms-data-breach-impacts-majority-of-14-million-customers/).
[25] *Id.*

43. While Defendant has declined to confirm who the threat actor is and whether it is or is not being extorted, ShinyHunters has a history of conducting similar high-profile data breaches—including those against PowerSchool and SnowFlake, impacting Santander, Ticketmaster, AT&T, Advance Auto Parts, Neiman Marcus, and Cylance.[26]

44. Defendant knew it was storing and permitting its employees to use a CRM and its internal network service to transmit valuable and highly sensitive Private Information and that, as a result, Defendant's systems would be attractive targets for cybercriminals.

45. Defendant also knew that a breach of its system, and exposure of the information therein, would result in the increased risk of identity theft and fraud against the individuals whose Personal Information were compromised.

46. Defendant knew or should have known that immediate action was necessary to mitigate the access and disclosure of the Personal Information entrusted to it. However, it failed to do so and caused Plaintiff's and Class Members' highly sensitive information to be exposed to the public.

47. These risks are not theoretical. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issues a warning to potential targets, so they are aware of, and prepared for, a potential attack.

[26] *Id.*

48. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021. [27]

49. The United States Office for Civil Rights established, as part of the department of Health and Human Services ("HHS"), a "Breach Portal" to address the widespread issue of data breach.

50. Upon information and belief, Defendant was aware of the Data Breach as early as July 17, 2025. It therefore waited nine days before reporting it over a weekend. Importantly, this Data Breach was actually disclosed to the public by the press, as Defendant only sent notice to certain government agencies and without an accompanying sample notice to affected individuals.

51. Defendant still has yet to provide notice of the breach to affected policyholders.

52. The extent of Defendant's efforts to help Plaintiff and Class Members protect themselves is nominal: Defendant has offered to provide affected individuals 24 months of credit monitoring and identity theft protection.[28]

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

---

[27] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, INSURANCE INFORMATION INSTITUTE, (https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20).

[28] Emma Woollacott, *Everything we know about the Allianz Life data breach so far*, IT PRO (July 28, 2025) (https://www.itpro.com/security/data-breaches/everything-we-know-about-the-allianz-life-data-breach-so-far).

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

54. Personal Information is a valuable property right.[29] The value of Private Information as a commodity is measurable.[30] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[31] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[32] It is so valuable to identity thieves that once Private Information has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

55. As a result of their real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, Personal Information and other sensitive information directly on various Internet websites, making the information publicly available. This information from various

---

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

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

[31] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

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

breaches, including the information exposed in the Data Breach, can be aggregated, and becomes more valuable to thieves and more damaging to victims.

56. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[33]

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

58. Further, according to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals target "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 713 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights]

[33] United States Government Accountability Office, *Report to Congressional Requesters, Personal Information, June 2007*, (https://www.gao.gov/new.items/d07737.pdf).

OCR—an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[34]

B. Defendant Knew It Was at High Risk for a Data Breach

59. Beyond these statistics regarding the increasingly high incident rate of data breaches, Defendant had actual knowledge that it was at high risk for targeting by cybercriminals.

60. Defendant issued a report35 and accompanying press release36 in October of 2024 in which it acknowledged that "[f]requency and value of large cyber insurance claims up 14% and 17% year-on-year in the first half of 2024, with data and privacy breach-related elements present in two thirds of these losses".[37]

61. Indeed, Michael Daum—Global Head of Cyber Claims for Allianz Commercial—notes that a "rise in ransomware attacks including data exfiltration is a consequence of changing attacker tactics and the growing interdependencies between organizations sharing ever more volumes of personal records."[38]

---

[34] Steve Alder, "Editorial: Why Do Criminals Target Medical Records", The HIPAA Journal (https://www.hipaajournal.com/why-do-criminals-target-medical-records/) (Nov. 2, 2023).
[35] *Cyber security resilience 2024* (https://commercial.allianz.com/news-and-insights/reports/cyber-risk-trends.html)
[36] *New data privacy trends help drive growth in frequency and severity of large cyber claims: Allianz* (Oct. 9, 2024) (https://commercial.allianz.com/news-and-insights/news/cyber-risk-trends-2024.html).
[37] *Id.*
[38] *Id.*

62. The press release goes on to note that "many data breaches, including some of the largest mass data exfiltration cyber-attacks over the past 18 months, are the result of weak cyber security within organizations."[39]

63. Critically, Rishi Baviskar—Global Head of Cyber Risk Consulting for Allianz Commercial—is quoted as saying that "[e]arly detection and response capabilities are […] key."[40]

64. Defendant's "Cyber security resilience 2024" Report specifically identifies data exfiltration as an increasingly common feature of cyber attacks, with the goal of stealing personal and commercial sensitive data.[41]

65. It also points out that even if backed up, the data "is effectively lost as the attackers have a copy and will threaten to publish on the dark web."[42]

66. The Report notes that organizations are even more susceptible to data breaches as they become increasingly reliant on connected services that allow the exchange and share of data across entities, and that cyber criminals are now targeting these digital supply chains to exfiltrate personal data en masse.[43]

67. As evidenced by the Report, Defendant was acutely aware of the risk of breach and exfiltration of data, including Plaintiff's and Class Members' highly sensitive Personal Information.

---

[39] *Id.*
[40] *Id.*
[41] "Cyber security resilience 2024", at 9 (Oct., 2024) (https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/cyber-security-trends-2024.pdf)
[42] *Id.*
[43] *Id.* at 19.

68. Even more poignantly, the Report contains an entire section titled "Cyber hygiene", dedicated to "improving data protection and privacy."[44]

69. This section of the Report identifies phishing and stolen and/or compromised credentials as the two most commonly exploited security vulnerabilities, closely followed by cloud misconfiguration.

70. Defendant's Report describes various measures necessary for proper cyber security, including strong access controls, database segregation, backups, patching and training.[45] Defendant also recommends data breach simulations, which can identify gaps and weaknesses in a company's cyber security, breach response, and crisis management.[46]

71. Finally, Defendant recognized the importance of limited data retention[47]:

> Data breach and privacy risks can be mitigated in large part by good data governance and housekeeping, explains **Marisa Anthony, Senior Complex Claims Analyst, Allianz Commercial.**
>
> *"Be mindful of what data you are collecting. Only collect and store personal data that is needed for business purposes, not what you think you need, and have a process in place to dispose of that data when you no longer need it. This is a simple measure companies – large and small – can take that is low cost and doable today,"* says **Anthony.**

[44] *Id.* at 24.
[45] *Id.* at 26.
[46] *Id.*
[47] *Id.* at 27.

72. Despite having actual knowledge of both the high risk posed by data breach and the steps necessary to prevent and mitigate damage stemming from a data breach, Defendant failed to secure its systems against the cyber attack it suffered on July 16, 2025.

C. Defendant Failed to Implement Sufficient Cybersecurity Measures

73. Defendant did not have adequate cybersecurity monitoring systems in place to prevent unauthorized access to its networks.

74. "Cybersecurity or process monitoring also involves continuously observing and analyzing your computer network or systems to prevent cyberattacks. The primary objective of monitoring in cybersecurity is quickly identifying signs of vulnerability and responding to potential security threats in real-time."[48]

75. The Data Breach should have been noticed by Defendant through proper endpoint and network monitoring and scanning.

76. The attackers exfiltrated a massive amount of Personal Information. Such actions should have only been possible by Defendant network administrators and should have required even administrators to pass additional security features. Such exfiltration activity should have been detected and raised numerous red flags to Defendant had it properly monitored its system.

77. Had Defendant implemented adequate cybersecurity monitoring, the Data Breach would have been prevented or much smaller in scope.

[48] *Cyber Security Monitoring: Definition and Best Practices*, SentinelOne (Oct. 16, 2024), https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-monitoring/.

78. Defendant should have employed IP whitelisting. "One of the simplest yet effective methods of safeguarding systems is through IP whitelisting. It is particularly beneficial for businesses that rely on remote access or have distributed teams but want to maintain strict security protocols. . . . IP whitelisting is a security practice that involves creating a list of trusted IP addresses granted access to a specific server, application, or network. By using IP whitelisting, only pre-approved IP addresses can interact with your system. By restricting access to a select group of devices based on their IP addresses, you can limit exposure to potential attacks and unauthorized access. The method effectively controls access to critical business systems, cloud infrastructure, and online services."[49]

79. The United States Dept. of Commerce has also produced guidance for application whitelisting, NIST Special Publication 800-167: *Guide to Application Whitelisting,* which provides specific guidance to companies on how to implement whitelisting, to prevent "installation and/or execution of any application that is not specifically authorized for use on a particular host. This mitigates multiple categories of threats, including malware and other unauthorized software."[50]

80. Defendant also failed to follow its own guidelines as to what to do in the aftermath of a data breach.

[49] Timothy Shim, *IP Whitelisting: The Beginner's Guide*, Rapid Seedbox, (Oct. 7, 2024), https://www.rapidseedbox.com/blog/ip-whitelisting.

[50] *NIST Special Publication 800-167, Guide to Application Whitelisting*, NIST (Oct. 2015), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf.

81. According to an article on Defendant's website titled "Cyber: dealing with a data breach,"[51] taking immediate action is the most important step in a robust response to a data breach. Defendant states that there is a "critical moment" for action—"perhaps only a few minutes or maybe an hour or two at most". It is therefore essential that a trained response team has prepared for critical scenarios and clearly understands their roles and responsibilities.

82. Defendant has not made public what steps, if any, it took after discovering the breach on July 17, 2025, besides notifying the FBI.[52]

83. Defendant lists clear communication as the next step in responding to a data breach: the "response team must oversee…a comprehensive communications plans that reaches all affected audiences."[53]

84. What is clear, however, is that Defendant failed to communicate clearly with anyone after the Data Breach, including Plaintiff or the Class Members.

85. Defendant discovered the breach on July 17, 2025, one day after the breach occurred.[54] Defendant, however, did not announce the breach until July 26, 2025. This allowed for a nine-day period in which cybercriminals were able to expose Plaintiff's and the Class Members' data to the public, unbeknownst to Plaintiff and the Class Members.

---

[51] *Cyber: dealing with a data breach* (April 2023) (https://commercial.allianz.com/news-and-insights/expert-risk-articles/cyber-data-breach.html).
[52] *Reuters, Allianz Life says majority of US customers' data stolen in hack* (July 26, 2025) (https://www.bleepingcomputer.com/news/security/allianz-life-confirms-data-breach-impacts-majority-of-14-million-customers/).
[53] *Id.*
[54] *Reuters, Allianz Life says majority of US customers' data stolen in hack* (July 26, 2025) (https://www.reuters.com/technology/allianz-life-says-majority-us-customers-data-stolen-hack-2025-07-26/).

86. This means that from July 17 to July 26, 2025, Plaintiff and Class Members lost valuable time to guard against the misuse of their stolen Personal Information. During these nine days, Plaintiff and Class Members were robbed of the opportunity to freeze their credit cards, set up credit monitoring, or change their credentials. Because of Defendant's failure to communicate with the affected individuals, Plaintiff's and Class Members' injuries stemming from the Data Breach increased substantially in severity.

87. To date, Defendant still has not issued a notice to affected individuals.[55]

D. The Dark Web

88. It is likely or at least a real risk that Plaintiff and Class Members' information has been exposed or will be listed for sale on the "dark web".

89. The dark web is a part of the World Wide Web that is not accessible through traditional internet browsers. The term "dark web" is used to distinguish from the "clear web," the part of the World Wide Web that is readily accessible through traditional internet browsers. The dark web is accessed through The Onion Router ("Tor"), a privacy-focused communication system designed to enable anonymous internet browsing. It achieves this by routing web traffic through multiple volunteer-operated servers (relays), encrypting data at each step to ensure that both the user's location and browsing activity are difficult to trace. Tor uses a technique called "onion routing," where data is encrypted in layers like an onion. Each relay in the network peels away a layer of encryption before passing the

[55] Lawrence Abrams, Allianz Life confirms data breach impacts majority of 1.4 million customers (July 26, 2025) (https://www.bleepingcomputer.com/news/security/allianz-life-confirms-data-breach-impacts-majority-of-14-million-customers/)

data to the next relay. This ensures that no single relay knows both the origin and destination of the data.

90. The dark web poses significant challenges to cyber security professionals and law enforcement agencies. The dark web is legal to access and operate, and it has some legitimate applications and sites. But its hidden nature and employment of multi-level encryption make detecting and monitoring illegal activity difficult. Unlike the clear web, dark web sites do not advertise their existence. The anonymity of the dark web has led to the creation of a number of markets and forums which traffic in illegal merchandise and content, including stolen Personal Information.[56]

91. Once stolen Personal Information is posted on the dark web, it will most likely be distributed to multiple different groups and individuals, each of which can use that information for fraud and identity theft.[57]This data lifecycle has also been confirmed with experiments. In 2015, researchers at BitGlass created a list of 1,568 phony names, Social Security numbers, credit card numbers, addresses, and phone numbers, rolled them in an Excel spreadsheet, and then "watermarked" it with their code that silently tracks any access to the file.[58] The data was quickly spread across five continents: North America,

[56] *Crime and the Deep Web*, STEVENSON UNIV. (https://www.stevenson.edu/online/about-us/news/crime-deep-web/); *Defending Against Malicious Cyber Activity Originating from Tor*, CISA, (https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-183a).
[57] *The Dark Web and Cybercrime*, U.S. Dep't of Health and Human Servs. (July 23, 2020), (https://www.hhs.gov/sites/default/files/dark-web-and-cybercrime.pdf).
[58] Kelly Jackson Higgins, *What Happens When Personal Information Hits the Dark Web*, Dark Reading (Apr. 7, 2015), (https://www.darkreading.com/cyberattacks-data-breaches/what-happens-when-personal-information-hits-the-dark-web); Kristin Finklea, *Dark Web*, Nat'l Sec. Archive (July 7, 2015), (https://nsarchive.gwu.edu/media/21394/ocr); *Dark Web*, Congressional Research Service, (https://crsreports.congress.gov/product/pdf/R/R44101) (last updated Mar. 10, 2017).

Asia, Europe, Africa, and South America. In the end, it was downloaded by 47 different parties. It was mainly downloaded by users in Nigeria, Russia, and Brazil, with the most activity coming from Nigeria and Russia.[59] This experiment demonstrated that data released on the dark web will quickly spread around the world.

E. Effects of the Data Breach

92. Personal Information is valuable property. Its value is axiomatic, considering the market value and profitability of "Big Data" to corporations in America. Illustratively, Alphabet Inc., the parent company of Google, reported in its 2020 Annual Report a total annual revenue of $182.5 billion and net income of $40.2 billion.[60] $160.7 billion of this revenue derived from its Google business, which is driven almost exclusively by leveraging the Personal Information it collects about users of its various free products and services. Criminal law also recognizes the value of Personal Information and the serious nature of the theft of Personal Information by imposing prison sentences. This strong deterrence is necessary because cybercriminals extract substantial revenue through the theft and sale of Personal Information. Once a cybercriminal has unlawfully acquired Personal Information, the criminal can demand a ransom or blackmail payment for its destruction, use the Personal Information to commit fraud or identity theft, or sell the Personal Information to other cybercriminals on the black market.

---

[59] Pierluigi Paganini, *How Far Do Stolen Data Get in the Deep Web After a Breach?*, Security Affairs (Apr. 12, 2015), (https://securityaffairs.com/35902/cyber-crime/propagation-data-deep-web.html).

[60] *Alphabet Inc., Annual Report (Form 10-K)*, SEC, at 32 (Feb. 3, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001652044/000165204421000010/goog-20201231.htm.

93. The U.S. Government Accountability Office ("GAO") released a report as far back as 2007 regarding data breaches, finding that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[61] This has not changed over the nearly two decades since this study.

94. The GAO Report explains that "[t]he term 'identity theft' is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name." Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[62] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to, among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw

[61] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* ("GAO Report") at 2, GAO (June 2007), (https://www.gao.gov/assets/270/262899.pdf) [https://perma.cc/GCA5-WYA5].

[62] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things: "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number. *Id*.

funds; obtain a new driver's license or ID; or use the victim's information in the event of arrest or court action.[63]

95. With access to an individual's Personal Information, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and Social Security number to obtain government benefits; filing a fraudulent tax return using the victim's information; or committing healthcare fraud using information related to an individual's health insurance. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[64]

96. Identity theft presents many challenges. In a survey, the Identity Theft Resource Center ("ITRC") found that most victims of identity crimes need more than a month to resolve issues stemming from identity theft and some need over a year.[65]

97. Theft of Social Security numbers creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new Social Security number, a breach victim has to demonstrate ongoing harm from misuse of their

---

[63] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Private Information and How Can You Protect Yourself*, Experian (May 21, 2023), (https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/).

[64] *Id.*

[65] *ITRC Annual Data Breach Report 2023*, ITRC (2023), (https://www.idtheftcenter.org/publication/2023-data-breach-report/).

Social Security number, and a new Social Security number will not be provided until after the victim experiences the harm.

98. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other PII (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity.

99. Beyond monetary losses and healthcare fraud, data breaches also have a deep, psychological impact on their victims.

> *In some ways, a cyber attack can feel like the digital equivalent of getting robbed, with a corresponding wave of anxiety and dread. Anxiety, panic, fear, and frustration—even intense anger—are common emotional responses when experiencing a cyber attack. While expected, these emotions can paralyze you and prolong or worsen a cyber attack.*[66]

100. Plaintiff and Class Members have suffered injuries in a number of ways, including:

- Loss of benefit of their bargain, for individuals who provided compensation to entities to safely transfer and store their data with Defendant or Defendant's vendors;
- Loss of value of their personal information, in that it has been misused for purposes to which they did not consent, and they have not been properly compensated for this misuse;

[66] Amber Steel, *The Psychological Impact of Cyber Attacks*, LastPass (Aug. 17, 2022), (https://blog.lastpass.com/posts/the-psychological-impact-of-cyber-attacks).

- Actual or attempted fraud, misuse, or identity theft caused by the Data Breach, including, but not limited to, their information being published to the clear, deep, and dark web; as well as

- Time and expenses that were reasonably spent to mitigate the impact of the breach, including the cost of credit monitoring.

101. Plaintiff and Class Members have already experienced actual or attempted fraud, which is reasonably related to the Data Breach, and which demonstrates that the Data Breach has put them at immediate risk for additional harm.

102. The fraud and attempted fraud that certain Plaintiff and Class Members have suffered is sufficiently related to the Data Breach because of the time frame in which it occurred (after the Data Breach), and because the same information that was exposed in the Data Breach would have been used to effectuate the fraud and identity theft.

103. The harm already suffered by Plaintiff demonstrates that the risk of harm to Plaintiff and Class Members is present and ongoing.

F. It Is Reasonable for Individual Victims of Data Breaches to Expend Time and Money to Mitigate Their Risk of Harm

104. Cybercriminals can and do use the precise Personal Information that Defendant was entrusted to safeguard to perpetrate financial crimes that harm Plaintiff and the Class Members.

105. The Federal Trade Commission ("FTC") recommends that identity theft victims take several steps to protect their Personal Information after a data breach, including contacting one of the three credit bureaus to place a fraud alert (and to consider an extended fraud alert that lasts for seven years if identity theft occurs), reviewing their

credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[67]

106. There may also be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Personal Information is stolen and when it is used. According to the GAO Report: "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[68]

107. Personal Information is such an inherently valuable commodity to identity thieves that, once it is compromised, criminals often trade the information on the cyber black-market for years.

108. Theft of PII is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[69]

---

[67] *Identity Theft Recovery Steps*, FTC, (https://www.identitytheft.gov/Steps). Indeed, the FTC takes data breaches seriously, and has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information can constitute an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

[68] GAO Report, *supra*, n.61.

[69] Patrick Lucas Austin, "*It Is Absurd." Data Breaches Show It's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019, 3:39 PM), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

109. Medical identity theft "is also more difficult to detect, taking almost twice as long as normal identity theft."[70] In warning consumers of the dangers of medical identity theft, the FTC states that an identity thief may use Personal Information "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[71] The FTC also warns, "[i]f the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[72]

110. There may be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. On average, it takes approximately three months for a consumer to discover their identity has been stolen and used and it takes some individuals up to three years to learn that information.[73]

111. A report published by the World Privacy Forum[74] and presented at the U.S. FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters.

[70] Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, World Privacy Forum (Dec. 12, 2017), (https://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf).
[71] *See* FBI, Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain (Apr. 8, 2014) at 14, (https://publicintelligence.net/fbi-health-care-cyber-intrusions/).
[72] *See* What to Know About Medical Identity Theft, FTC, (https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft).
[73] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 J. of Systemics, Cybernetics and Informatics 9 (2019), (http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf).
[74] Dixon & Emerson, *supra*, n. 70.

These changes can affect the healthcare a person receives if the errors are not caught and corrected.

- Significant bills for medical goods and services not sought or received.

- Issues with insurance, co-pays, and insurance caps.

- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.

- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime.

- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgages or other loans and may experience other financial impacts.

- Phantom medical debt collection based on medical billing or other identity information.

- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.

112. Furthermore, data breaches that expose any personal data, and in particular non-public data of any kind (e.g., donation history or hospital records), directly and materially increase the chance that a potential victim is targeted by a spear phishing attack in the future, and spear phishing results in a high rate of identity theft, fraud, and extortion.[75]

[75] *See* Leo Kelion & Joe Tidy, *National Trust Joins Victims of Blackbaud Hack*, BBC News (July 30, 2020), (https://www.bbc.com/news/technology-53567699) (concluding that personal information such as "names, titles, telephone numbers, email addresses, mailing addresses, dates of birth, and, more importantly, donor information such as donation dates, donation amounts, giving capacity, philanthropic interests, and other donor profile information . . . in the hands of fraudsters, [makes consumers] particularly susceptible to spear phishing—a fraudulent email to specific targets while purporting to

113. Plaintiff and Class Members' stolen data will continue to be leaked and traded on the dark web, meaning Plaintiff and Class Members will remain at an increased risk of fraud and identity theft for many years into the future. Indeed, some Class Members are in the very early stages of their lives—in their twenties and thirties. Thus, as the respective Data Breach Notices advise, customers, including Plaintiff and Class Members, must vigilantly monitor their financial accounts for many years to come.

G. Damages Can Compensate Victims for the Harm Caused by the Data Breach

114. Defendant has refused to provide adequate compensation for Plaintiff's and Class Members' injuries.

115. The Personal Information exposed in the Data Breach has real value, as explained above. Plaintiff and the Class Members have therefore been deprived of their rights to control of that property and have lost the value they might otherwise have incurred from that data.[76]

116. Plaintiff and the Class Members have already spent significant time, and will spend much more, monitoring their accounts, changing login credentials, and recovering from the inevitable fraud and identity theft which will occur, which deserves to be

be a trusted sender, with the aim of convincing victims to hand over information or money or infecting devices with malware").

[76] Ravi Sen, *Here's How Much Your Personal Information Is Worth to Cybercriminals – and What They Do with It*, PBS (May 14, 2021), (https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it).

compensated. Defendant has not made compensation or other remedies available for these very real injuries.[77]

117. Similarly, Defendant has offered no compensation for the aggravation, agitation, anxiety, and emotional distress that Plaintiff and the Class Members have suffered, and will continue to suffer, as a result of the Data Breach: the knowledge that their information is out in the open, available for sale and exploitation at any time in the future is a real harm that also deserves compensation.

118. Plaintiff and Class Members were also deprived of the benefit of their bargain when they interacted with Defendant: Defendant had a duty to take reasonable steps to protect the Personal Information of the individuals whose information was entrusted to them and those individuals entrusted that information in exchange for Defendant taking on that duty. This duty was inherent in the relationships between Plaintiff and Class Members and Defendant, whether through express contractual terms, implied contractual terms, bailment, or statutory or implied duties of good faith and fair dealing.

119. Defendant has not taken sufficient steps or even attempted to make impacted patients whole. Defendant has failed their duty to protect Plaintiff's and Class Members' Personal Information and have failed in their duty to help these consumers protect themselves in the future.

[77] Time spent monitoring accounts is another common and cognizable, compensated harm in data breach cases. *See Equifax Data Breach Settlement*, FTC, https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement (last visited Nov. 26, 2024).

H. Defendant Breached Its Duty to Protect Plaintiff's and Class Members' Private Information

120. Defendant's cybersecurity practices and policies were inadequate and fell short of the industry-standard measures that should have been implemented long before the Data Breach occurred.

121. However, because Defendant markets and advertises itself as securely handling highly sensitive Personal Information, Defendant assumed legal and equitable duties and knew or should have known it was responsible for:

- adequately designing, maintaining, and updating their software and networks;
- promptly detecting, remediating, and notifying their customers of any critical vulnerabilities in their software and networks;
- ensuring compliance with industry standards related to data security;
- ensuring compliance with regulatory requirements related to data security;
- protecting and securing the Personal Information stored on their networks from unauthorized disclosure; and
- providing adequate notice to customers and individuals if their Personal Information is disclosed without authorization.

122. Defendant failed to use the requisite degree of care that a reasonably prudent company would use in designing, developing, and maintaining networks that store highly sensitive Personal Information.

123. Defendant should have implemented industry standard security protocols to mitigate the risk of a Data Breach.

124. In addition to mitigating the risk of stolen credentials, the Cybersecurity and Infrastructure Security Agency (CISA) guidance encourages organizations to prevent unauthorized access by:

- adequately designing, maintaining, and updating their software and networks;
- promptly detecting, remediating, and notifying their customers of any critical vulnerabilities in their software and networks;
- ensuring compliance with industry standards related to data security;
- ensuring compliance with regulatory requirements related to data security;
- protecting and securing the Personal Information stored on their networks from unauthorized disclosure; and
- providing adequate notice to customers and individuals if their Personal Information is disclosed without authorization.

125. The CISA guidance further recommends use of a centrally managed antivirus software utilizing automatic updates that will protect all devices connected to a network (as opposed to requiring separate software on each individual device), as well as implementing a real-time intrusion detection system that will detect potentially malicious network activity that occurs prior to ransomware deployment.[78] Likewise, the principle of least privilege ("POLP") should be applied to all systems so that users only have the access they need to perform their jobs.[79]

126. Not only should Defendant have had measures like these in place to prevent compromise in the first place, Defendant should have also properly siloed their systems so

[78] *Id.* at 5.
[79] *Id.* at 6.

that a bad actor would be unable to escalate privileges and move laterally through Defendant's systems.

127. Defendant's lack of segmented systems, which are common to cloud-based servers, allowed the hacker to travel among Defendant's systems freely, compromising multiple systems which Defendant was unable to recover.

128. CISA guidance recommends that using a comprehensive network, in addition to network segregation, will help contain the impact of an intrusion and prevent or limit lateral movement on the part of malicious actors.

129. Despite holding the Personal Information of millions of patients, Defendant failed to adhere to these recommended best practices. Indeed, had Defendant implemented common sense security measures, the hackers never could have accessed millions of patient files and the Data Breach would have been prevented or been much smaller in scope. Defendant also lacked the necessary safeguards to detect and prevent phishing attacks and failed to implement adequate monitoring or control systems to detect the unauthorized infiltration after it occurred.

130. Defendant, like any entity their size storing valuable data, should have had robust protections in place to detect and terminate a successful intrusion long before access and exfiltration could expand to millions of patient files. Defendant's below-industry-standard procedures and policies are inexcusable given their knowledge that they were a prime target for cyberattacks.

131. Defendant's failure to follow industry standard cybersecurity protocols directly resulted in the Data Breach and the compromise of Plaintiff's and Class Members' Personal Information.

I. Defendant Failed to Follow Industry Standards for Data Security

132. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[80]

133. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal 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.[81]

134. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[82]

---

[80] *Start with Security: A Guide for Business*, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[81] *Protecting Personal Information: A Guide for Business,* FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[82] *Id.*

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

136. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, 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, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[83]

137. Defendant was fully aware of their obligation to implement and use reasonable measures to protect the Personal Information of their patients but failed to comply with these basic recommendations and guidelines that would have prevented this breach from occurring. Defendant's failure to employ reasonable measures to protect against unauthorized access to patient information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

J. HIPAA Obligations

138. Defendant is covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (*see* 45 C.F.R. § 160.102) and as such are required to comply with

[83] *Privacy and Security Enforcement*, FTC, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement (last visited Jan. 13, 2025).

the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

139. These rules establish national standards for the protection of patient information, including personal health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. 45 C.F.R. § 160.103.

140. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."[84]

141. HIPAA requires that Defendant implement appropriate safeguards for this information.[85]

142. HIPAA requires that Defendant provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons—i.e., non-encrypted data.[86]

[84] 45 C.F.R. § 164.502.
[85] 45 C.F.R. § 164.540(c)(1).
[86] 45 C.F.R. §§ 164.402, 404.

143. HIPAA further requires covered entities to "[i]mplement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed." [87]

144. HIPAA security standards require organizations to "[p]rotect against any reasonably anticipated threats or hazards to the security or integrity of such information."[88] Automatically tracking IoC's is a recommended practice.[89]

145. It is also recommended to use an Intrusion Prevention System (IPS) and in order "[t]o stay up to date, IPS should leverage a Structure Threat Information eXpression (STIX)/Trusted Automated eXchange of Indicator Information (TAXII) feed to obtain IOC from an Information Sharing and Analysis Center (ISAC) or similar source."[90]

146. Having systems in place for continuous monitoring for IoCs is also recommended.[91]

147. As evidenced by the Data Breach, Defendant did not track IoCs.

---

[87] 45 C.F.R. § 164(c).
[88] 45 C.F.R. § 164.306.
[89] Robert Brzezinski, *HIPAA Privacy and Security Compliance - Simplified: Practical Guide for Small and Medium Organizations* 28 (2016 ed.)
[90] *Technical Vol. 2: Cybersecurity Practices for Medium and Large Healthcare Organizations 2023 Edition*, Healthcare & Public Health Sector Coordinating Council, U.S. Dept. of Health & Human Services, (https://405d.hhs.gov/Documents/tech-vol2-508.pdf).
[91] *SecurityMetrics Guide to HIPAA Compliance*, SecurityMetrics (8th ed. 2023), ("Automating log collection, correlation and review to Detect Indicators of Attack (IoA) and Indicators of Compromise (IoC). Security Incident and Event Management (SIEM) tools are a good way to automate the process even for small companies.").

148. Despite the requirements under HIPAA for data security, Defendant failed to comply with their duties under HIPAA and their own privacy policies. Indeed, Defendant failed to:

a. Maintain an adequate data security system to reduce the risk of data breaches and cyberattacks;

b. Adequately protect the Personal Information of policyholders;

c. Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

d. Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. § 164.312(a)(1);

e. Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1)(i);

f. Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

g. Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

h. Ensure compliance with the electronically protected health information security standard rules by their workforces, in violation of 45 C.F.R. § 164.306(a)(4); and/or

i. Train all members of their workforces effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of their workforces to carry out their functions and to maintain security of protected health information, in violation of 45 C.F.R. § 164.530(b).

149. NIST 800-53 also recommends removing, masking, encrypting, or hashing PII contained in company datasets.[92]

> There are many possible processes for removing direct identifiers from a dataset. Columns in a dataset that contain a direct identifier can be removed. In masking, the direct identifier is transformed into a repeating character, such as XXXXXX or 999999. Identifiers can be encrypted or hashed so that the linked records remain linked. In the case of encryption or hashing, algorithms are employed that require the use of a key, including the Advanced Encryption Standard or a Hash-based Message Authentication Code. Implementations may use the same key for all identifiers or use a different key for each identifier. Using a different key for each identifier provides a higher degree of security and privacy.

[92] *NIST Special Publication 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations*, Natl. Institute of Standards and Tech., U.S. Dept. of Commerce, (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf).

> Identifiers can alternatively be replaced with a keyword, including transforming "George Washington" to "PATIENT" or replacing it with a surrogate value, such as transforming "George Washington" to "Abraham Polk."[93]

150. Given the attackers were able to access Personal Information simply by logging in, it is clear that Defendant did not protect Plaintiff's and Class Members' Personal Information with sufficient masking, encrypting, or hashing.

151. Defendant was fully aware of their obligations to implement and use reasonable measures to protect the Personal Information of patients but failed to comply with these basic recommendations and guidelines that would have prevented this Data Breach from occurring. Defendant's failure to employ reasonable measures to protect against unauthorized access to patient Personal Information violated HIPAA and constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

K. Plaintiff and Class Members Suffered Damages

152. Defendant received Plaintiff's and Class Members' Private Information in connection with providing certain financial services to them. In requesting and maintaining Plaintiff's Private Information for business purposes, Defendant expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff's and Class Members' Private Information. Defendant did not, however, take proper care of Plaintiff's and Class Members' Private Information, leading to its exposure to and exfiltration by cybercriminals as a direct result of Defendant's inadequate security measures.

[93] *Id.*

153. For the reasons mentioned above, Defendant's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class Members significant injuries and harm in several ways. Plaintiff and Class Members must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them. Plaintiff and Class Members have taken or will be forced to take these measures in order to mitigate their potential damages as a result of the Data Breach.

154. Once Personal Information is exposed, there is little that can be done to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct.

155. Further, the value of Plaintiff and Class Members' Private Information has been diminished by its exposure by the Data Breach. Plaintiff and Class Members did not receive the full benefit of their bargain when paying for financial services, and instead received services that were of a diminished value to those described in their agreements with Defendant for the benefit and protection of Plaintiff and Class Members and their respective Private Information. Plaintiff and Class Members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for

(which would have included adequate data security protection) and the services they received.

156. Plaintiff and Class Members would not have obtained services from Defendant or paid the amount they did to receive such services, had they known that Defendant would negligently fail to protect their Private Information. Indeed, Plaintiff and Class Members paid for services with the expectation that Defendant would keep their Private Information secure and inaccessible from unauthorized parties. Plaintiff and Class Members would not have obtained services from Defendant had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Personal Information from criminal theft and misuse.

157. As a result of Defendant's failures, Plaintiff and Class Members are also at substantial and certainly impending increased risk of suffering identity theft and fraud or other misuse of their Personal Information.

158. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[94]

159. Plaintiff and Class Members are also at a continued risk because their information remains in Defendant's computer systems, which have already been shown to

[94] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KNOWBE4, (https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud).

be susceptible to compromise and attack and is subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its consumers' Personal Information.

160. In addition, Plaintiff and Class Members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial and/or medical fraud, and the unauthorized exposure of their private information to strangers.

CLASS ALLEGATIONS

161. Plaintiff brings this action pursuant to Fed. R. Civ. P. 23(a), 23(b)(2), and (23(b)(3), individually and on behalf of all members of the following nationwide class:

> **Nationwide Class:** All residents of the United States and its Territories who had their Personal Information compromised due to the Data Breach.

162. Excluded from the Class are Defendant's officers and directors; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

163. Plaintiff reserves the right to amend or modify the Class definitions.

164. **Numerosity**. The Class is so numerous that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiff. Defendant has confirmed that the Class consists of over 1.4 million United States residents residing in each State, totaling over one-third of the United States.

165. **Commonality**. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff and Class Members' Personal Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Personal Information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards and state and federal regulatory requirements, including HIPAA;

e. Whether Defendant was subject to and breached contractual obligations to adhere to HIPAA in their business association agreements;

f. Whether Defendant owed a duty to Plaintiff and Class Members to safeguard their Personal Information;

g. Whether Defendant breached their duties to Plaintiff and Class and Members to safeguard their Personal Information;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Defendant should have discovered the Data Breach earlier;

j. Whether Defendant's delay in issuing notice to Plaintiff and the Class caused them incremental harm;

k. Whether Plaintiff and Class members suffered legally cognizable damages as a result of Defendant's misconduct;

l. Whether Defendant's conduct was negligent;

m. Whether Defendant failed to provide notice of the Data Breach in a timely manner;

n. Whether Defendant was unjustly enriched due to their use of Plaintiff's and the Class's Personal Information while failing to protect it; and,

o. Whether Plaintiff and Class Members are entitled to damages, civil penalties, treble damages, and/or injunctive relief.

166. **Typicality**. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Personal Information, like that of every other Class Member, was compromised in the Data Breach, causing them common injury, which was due to the same misconduct—Defendant's inadequate data security.

167. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Class Members. Plaintiff's Counsel are competent and experienced in litigating class actions.

168. **Predominance**. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all of Plaintiff's and Class Members' Personal

Information was stored on the same computer system and unlawfully accessed by authorized users in the same way due to the same security deficiencies. Defendant's misconduct caused common injuries that affect all Class Members. Defendant's common course of wrongdoing and the common, classwide injuries create common legal and factual issues that predominate over any individualized issues. Adjudication of these common issues in a single action advances the interests of judicial economy.

169. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation concerning the same facts and law. Moreover, this case furthers the quintessential purpose of a class action, which is to afford Class Members with common injuries to pursue collective litigation where their individual damages are small. Given the size of the Plaintiff's and Class Members' individual damages, the costs of individual litigation would likely exceed any award, leaving Plaintiff and Class Members with effectively no remedy for their harm. Additionally, the prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications and establish incompatible standards of conduct for healthcare entities. In contrast, litigating this matter as a class action presents far fewer management difficulties, conserves judicial and party resources, and protects the rights of each Class Member.

170. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

CAUSES OF ACTION

COUNT I
Negligence
(On behalf of Plaintiff and the Nationwide Class)

171. Plaintiff re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

172. Defendant, via their business operations, collected, maintained, stored, used, analyzed, and processed Plaintiff's and the Class's highly private information, including personally identifying and medical information. Defendant collected this Personal Information as part of its efforts to further its profit and gain an advantage against its competitors.

173. Defendant understood the need to adequately protect that sensitive information and the serious risk a data breach poses to patients, such as Plaintiff and the Class. Defendant, furthermore, was subject to state and federal regulations, including HIPAA and state-law equivalents, that required Defendant to implement reasonable physical, technical, and administrative safeguards to protect patient information from unauthorized access, use, or disclosure.

174. Further, given the value of the private data to Defendant and its business model and the well-known misuse of Personal Information by cybercriminals, Defendant also fully understood that patient data has significant monetary value. Defendant knew or should have known that, should that sensitive data be accessed by unauthorized users, it would likely be sold on the dark web to fraudsters, putting patients, including Plaintiff and the Class Members, at significant risk that their Personal Information would be used for

fraudulent purposes. Indeed, the fact that Defendant *themselves* profited from the data that comprises Plaintiff's and the Class's Personal Information demonstrates that Defendant knew or should have known the importance of data security.

175. Given the highly sensitive nature of the data, and the foreseeable risk of a Data Breach, Defendant owed Plaintiff and the Class Members a duty to exercise reasonable care in securing the highly sensitive Personal Information, including a host of private medical data, that Defendant collected, maintained, stored, used, analyzed, and processes as part of their businesses.

176. Defendant owed this duty to Plaintiff and the Class Members because Plaintiff and the Class are a well-defined, and foreseeable group of individuals whom Defendant should have been aware could be injured by Defendant's inadequate data storage and security. The foreseeable harm to Plaintiff and the Class of Defendant's inadequate data security measures and the fact that Defendant was the only entity capable of protecting Plaintiff's and the Class's data within their possession created a duty to act reasonably in securing Personal Information.

177. Additionally, Defendant assumed a duty to Plaintiff and the Class to protect their sensitive Personal Information. Defendant represented that they would comply with HIPAA to implement measures to reasonably safeguard the sensitive information within their possession. As such, when intermediaries provided Defendant with Plaintiff's and the Class's Personal Information and Defendant accepted and stored that data (for their own purposes and to their own financial benefit), Defendant assumed a duty to protect that Personal Information.

178. Defendant also owed a duty to timely and accurately disclose the scope, nature, and occurrence of the Data Breach. This disclosure is necessary so Plaintiffs and the Class can take appropriate measures to avoid unauthorized use of their Personal Information and accounts, cancel and/or change usernames and passwords on compromised accounts, monitor their accounts to prevent fraudulent activity, contact their financial institutions about compromise or possible compromise, obtain credit monitoring services, and/or take other steps in an effort to mitigate the harm caused by the Data Breach and Defendant's unreasonable misconduct.

179. Despite this duty, Defendant did not implement reasonable data security and negligently maintained Plaintiff's and the Class's Personal Information. For example, Defendant lacked internal cybersecurity monitoring of Defendant's systems and failed to adequately segregate sensitive information from Defendant's other systems. Each of these failures contravenes well-established, basic industry standards, expert recommendations, and basic requirements for reasonable data security.

180. Defendant knew that its failure to use reasonable measures to protect Class Members' Personal Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the well-known high frequency of cyberattacks and data breaches in the past few years.

181. Defendant's negligent data security actually and proximately caused Plaintiff's and the Class's injuries because they directly allowed hackers to easily access Plaintiff's and the Class's Personal Information. This ease of access allowed the hackers

to steal Personal Information of Plaintiff and the Class, resulting in the dissemination of that data on the dark web.

182. As a direct and proximate result of Defendant's misconduct, Plaintiff and the Class have suffered theft of their Personal Information. Defendant allowed cybercriminals to access Class Members' Personal Information, thereby decreasing the security of the Class's financial and health accounts, making Class Members' identities less secure and reliable, and subjecting the Class to the imminent threat of identity theft. Not only will Plaintiff and the Class have to incur time and money to re-secure their bank accounts and identities, but they will also have to protect against identity theft for years to come.

183. As a direct and proximate result of Defendant's inadequate security and the resulting Data Breach, Plaintiff and Class Members suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (8) a continued substantial and imminent risk of the misuse of their Personal Information.

184. Plaintiff and the Class also remain at heightened risk of future injury because their Personal Information resides with Defendant and, further, because Defendant continues to gather new medical information on Plaintiff and the Class. Without the use of

adequate data security, Plaintiff and the Class remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

185. Plaintiff and the Class seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and which the court deems proper.

COUNT II

Negligence *Per Se*
(On behalf of Plaintiff and the Nationwide Class)

186. Plaintiff re-alleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

187. Pursuant to Section 5 of the Federal Trade Commission Act ("FTCA"), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Personal Information. 15 U.S.C. § 45.

188. Plaintiff and Class Members are within the class of persons that the FTCA was intended to protect.

189. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against. The FTC has pursued enforcement actions against businesses that, due to their failure to employ reasonable data security measures and abstain from unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class here.

190. As entities that receive health information, Defendant is a "business associate" under HIPAA. Business associates have legal obligations to implement administrative, technical, and physical safeguards. 42 U.S.C. § 17931 (applying security requirements to business associates and incorporating security requirements into business associate agreements ("BAAs") between business associates and covered entities); see also 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards); 42 U.S.C. § 17902.

191. Plaintiff and the Class, as patients, are within the class of people HIPAA was designed to protect and HIPAA was intended to protect Plaintiff and the Class against the type of harm that occurred, namely, unauthorized access to Plaintiff's and the Class's medical information.

192. Defendant's implementation of inadequate data security failed to comply with HIPAA, including because it: (i) failed to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and the Class's Personal Information; (ii) failed to adequately monitor Defendant's servers despite the vast amount of patient data stored there; (iii) failed to implement multi-factor authentication on remote access accounts; (iv) allowed unauthorized access to Plaintiff's and the Class's Personal Information; (iv) failed to detect in a timely manner the unauthorized access and exfiltration of patient data occurring in Defendant's systems; and (v) failed to timely and adequately notify Plaintiff and the Class of the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

193. Defendant knew that their inadequate data security measures put Plaintiff and the Class at foreseeable risk of harm from a data breach (including the Data Breach described in this Complaint) which, in turn, put Plaintiff at risk of harm due to the theft and misuse of their data.

194. As a direct and proximate result of Defendant's misconduct, Plaintiff and the Class have suffered theft of their Personal Information. Defendant allowed cybercriminals to access Class Members' Personal Information, thereby decreasing the security of the Class's financial and health accounts, making Class Members' identities less secure and reliable, and subjecting the Class to the imminent threat of identity theft. Not only will Plaintiff and the Class have to incur time and money to re-secure their bank accounts and identities, but they will also have to protect against identity theft for years to come.

195. As a direct and proximate result of Defendant's inadequate security and the resulting Data Breach, Plaintiff suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (8) a continued substantial and imminent risk of the misuse of their Personal Information.

196. Plaintiff and the Class also remain at heightened risk of future injury because their Personal Information resides with Defendant and, further, because Defendant continues to gather new information on Plaintiff and the Class. Without the use of adequate data security, Plaintiff and the Class remain at a heightened and substantial risk that their Personal Information will be subject to another data breach. Plaintiff and the Class seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT III

Third Party Beneficiary – Breach of Contract
(On behalf of Plaintiff and the Nationwide Class)

197. Plaintiff re-alleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

198. Plaintiff and Class Members have an interest, both equitable and legal, in the Personal Information about them that was conveyed to, collected by, and maintained by Defendant and that was ultimately accessed or compromised in the Data Breach.

199. As a recipient of employees', former employees', and business associates' Personal Information, Defendant has a fiduciary relationship to Plaintiff and the Class Members.

200. Because of that fiduciary relationship, Defendant was provided with and stored private and valuable Personal Informationrelated to Plaintiff and the Class. Plaintiff

and the Class were entitled to expect their information would remain confidential while in Defendant's possession.

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

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

203. Defendant had possession and knowledge of confidential PII of Plaintiff and Class Members, information not generally known.

204. Plaintiff and Class Members did not consent to nor authorize Defendant to release or disclose their Personal Information to unknown criminal actors.

205. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by, among other things: mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of employee information that resulted in the unauthorized access and compromise of Personal Information; mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; failing to design and implement information safeguards to control these risks; failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; failing to evaluate and adjust its information security program in light of the circumstances alleged herein; failing to detect

the breach at the time it began or within a reasonable time thereafter; failing to follow its own privacy policies and practices; and failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive Personal Information.

206. But for Defendant's wrongful breach of its fiduciary duties owed to Plaintiff and Class Members, their Personal Information would not have been compromised.

207. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff and Class Members have suffered injuries, including:

a. Theft of their Personal Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their Personal Information;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

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

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

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

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

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

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

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

209. Under HIPAA, a "business associate" is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provider of certain services to, a covered entity that involve access by the

business associate to PHI. HIPAA rules require that a covered entity and any business associate enter into an agreement (called a BAA, further described below) requiring the business associate to appropriately safeguard PHI.

210. Pursuant to HIPAA, a "business associate must comply with the applicable standards, implementation specifications, and requirements of [HIPAA] with respect to electronic protected health information of a covered entity." 45 C.F.R. § 164.302. Those safeguards include obligations to implement administrative, technical, and physical safeguards. 42 U.S.C. § 17931 (applying security requirements to business associates and incorporating security requirements into BAAs between business associates and covered entities); *see also* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards); 42 U.S.C. § 17902. These requirements are uniform and exist in every BAA.

211. Because each Defendant uses, analyzes, collets, obtains and accesses personal health information of patients, each must enter into Business Association Agreements ("BAA") with a covered entity, intermediatory, or other third party from whom Defendant obtains medical information. Through the normal course of their business, each Defendant obtains and uses personal health information, including Plaintiff's and the Class's Personal Information. Consequently, to have obtained access to and used Plaintiff's and the Class's Personal Information, Defendant must have entered into one or more BAA with one or more covered entities.

212. Those BAAs must each contain identical requirements obligating the signatories (*i.e.*, here, Defendant) to comply with HIPAA. The requirements in the BAA are intended to protect patients like Plaintiff's and the Class against the disclosure, theft, unauthorized access, or other harms stemming from the use of their medical information.

213. Although each Defendant was subject to a BAA and, therefore, HIPAA's requirements to implement adequate safeguards to protect patient information, Defendant failed to comply. Specifically, Defendant violated HIPAA and, thereby, breached their BAAs by, among other things, failing to adequately secure Plaintiff's and the Class's Personal Information, and failing to implement reasonable administrative, technical, and physical safeguards to protect Plaintiff's and the Class's Personal Information. Among other things, Defendant violated HIPAA by permitting access to servers containing Plaintiff's and the Class's unencrypted Personal Information without the use of MFA; failed to adequately segregate Plaintiff's and the Class's Personal Information; and failed to adequately monitor activity on the sever containing Plaintiff's and the Class's Personal Information.

214. As a direct and proximate result of Defendant's violation of HIPAA and breach of its required BAAs, Plaintiff and the Class suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft

and posting of their Personal Information; (7) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (8) a continued substantial and imminent risk of the misuse of their Personal Information.

215. Plaintiff and the Class also remain at heightened risk of future injury because their Personal Information resides with Defendant and, further, because Defendant continues to gather new information on Plaintiff and the Class via the direct or indirect contracts with policyholders. Absent compliance to those contracts' data security requirements, Plaintiff and the Class remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

216. Plaintiff and the Class seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

COUNT IV

Breach of Bailment
(On behalf of Plaintiff and the Nationwide Class)

217. Plaintiff re-alleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

218. Defendant, via their business operations, collected, maintained, stored, used, analyzed, and processed Plaintiff's and the Class's highly private information, including personally identifying and medical information. Defendant collected this Personal

Information as part of its efforts to further its profit and gain an advantage against its competitors.

219. As discussed *supra*, Personal Information is highly valuable. Plaintiff and Class Members delivered their Personal Information—i.e., a bailment—to Defendant with the understanding that Defendant would hold their Personal Information securely and for the specific and limited purpose of informing their policies and/or annuities.

220. A bailee such as Defendant has a legal duty (independent of any contractual duty) to exercise ordinary care to protect the subject of the bailment (Plaintiff's and Class Members' Personal Information) from negligent loss, damage, or destruction.

221. By accepting Plaintiff's and the Class Member's Personal Information, Defendants assumed a duty to faithfully secure Plaintiff's and Class Member's Personal Information while it remained in Defendant's possession.

222. Defendant understood the need to adequately protect that sensitive information and the serious risk a data breach poses to patients, such as Plaintiff and the Class. By accepting Plaintiff's and Class Members' Personal Information, Defendant assumed a duty to implement reasonable physical, technical, and administrative safeguards to protect Plaintiff's and Class Members' information from unauthorized access, use, or disclosure.

223. Because Defendant failed to fulfill their duty to protect Plaintiff's and Class Members' Personal Information, Defendant breached its bailment with Plaintiff and Class Members.

COUNT V

Unjust Enrichment
(On behalf of Plaintiff and the Nationwide Class)

224. Plaintiff re-alleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

225. Defendant received a substantial monetary benefit from Plaintiff and the Class by the collection, maintenance, and use (for their own benefit) of Plaintiff's Personal Information. Defendant has made substantial gains through the collection and analysis of Plaintiff's and the Class's Personal Information, which Defendant obtained under the promise of securing patient data from unauthorized access and to comply with HIPAA and other state and federal requirements to implement reasonable measures to protect that Personal Information.

226. Specifically, Defendant derived value by collecting, using, analyzing Plaintiff's and the Class's Personal Information. Upon information and belief, Defendant shared the information and analyses of it to other entities, thereby deriving a substantial benefit. Defendant, without any knowledge of the Plaintiff and the Class, had unfettered rights to use Plaintiff's and the Class's Personal Information for its own business profit.

227. Defendant further profited from the use, sharing, and analysis of Plaintiff's and the Class's Personal Information, which they used to maximize profit, increase their ability to compete with competitors, and obtain additional revenue at the expense of patients like Plaintiff and the Class.

228. Furthermore, Defendant saved money by: (1) devoting knowingly inadequate resources to securing Defendant's servers and networks despite its knowledge

that the servers were out of data and lacked adequate protections; and (2) failing to prioritize timely notifying Plaintiff and the Class that their Personal Information was impacted in the Data Breach, preventing Plaintiff and the Class for taking measures to protect against harm stemming from the misuse of their data.

229. Defendant would be unable to engage in their regular course of business without collecting the Personal Information from Plaintiff and the Class's medical providers.

230. Defendant's acceptance of the benefits of Plaintiff's and the Class's Personal Information under the facts and circumstances is unfair, unjust, and inequitable.

231. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiff and Class Members.

232. If Plaintiff and Class Members knew that Defendant had not secured their Personal Information or that they used their private medical information for their own financial gain, Plaintiff and the Class would not have agreed to provide their medical information to Defendant or to make unfettered use of that information, all while failing to implement reasonable safeguards to protect it.

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

234. Due to Defendant's unjust enrichment, Plaintiff suffered and will continue to suffer significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their

Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (8) a continued substantial and imminent risk of the misuse of their Personal Information.

235. Plaintiff and the Class also remain at heightened risk of future injury because their Personal Information resides with Defendant and, further, because Defendant continue to gather new medical information on Plaintiff and the Class. Without the use of adequate data security requirements, Plaintiff and the Class remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

236. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from the use of Plaintiff's and the Class's Personal Information.

COUNT VI

Declaratory Judgment
(On behalf of Plaintiff and the Nationwide Class)

237. Plaintiff re-allege and incorporates by reference the preceding paragraphs as if fully set forth herein.

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

239. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class Members' Personal Information and whether Defendant currently maintain data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their Personal Information.

240. Plaintiff allege that Defendant's data security measures remain inadequate. Plaintiff and Class Members will continue to suffer injury as a result of the compromise of their Personal Information and remain at imminent risk that further compromises of their Personal Information will occur in the future.

241. That risk stems from Defendant's retention of Plaintiff's Personal Information, and its continued collection and aggregation of new information in the normal course of business through Defendant's processing and resolution of insurance claims. Defendant, thus, will continue to receive new and additional information concerning Plaintiff and the Class and, consequently, Plaintiff and the Class remain at substantial risk of a subsequent breach resulting in the theft of additional Personal Information.

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

- Defendant continues to owe a legal duty to secure Plaintiff's and Class Members' Personal Information and to timely notify Plaintiff and Class Members of a data breach under the common law, Section 5 of the FTC Act, HIPAA, and various state statutes.

- Defendant continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiff's and Class Members' Personal Information.

243. The Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect Plaintiff's and Class Members' Personal Information.

244. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach. The risk of another data breach is real, immediate, and substantial. If another breach occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

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

246. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach of Defendant's systems, thus eliminating the additional injuries that would result to Plaintiff and the Class whose Personal Information would be further compromised.

COUNT VII

Violation of the Minnesota Deceptive Trade Practices Act ("MDTPA"), Minn. Stat. § 325D.43
(On Behalf of Plaintiff and the Nationwide Class)

247. Plaintiff, individually and on behalf of the Nationwide Class, re-allege and incorporate by reference the preceding paragraphs as if fully set forth herein.

248. Minnesota affords a cause of action to any person harmed by an entities use of deceptive trade practices. Minn. Stat. § 325D.45, Subd.3.

249. Under MDTPA, a "person engages in a deceptive trade practice when, in the course of business, vocation or occupation, the person . . . engaged in (i) unfair methods of competition, or (ii) unfair or unconscionable acts or practices[.]". Minn. Stat. § 325D.44, subd. 1(13).

250. Defendant engaged in conduct that violated the MDTPA.

251. Specifically, Defendant collected and stored Plaintiff's and the Class's Personal Information. Defendant stored the Personal Information in a knowingly unsafe and unsecured manner by, among other things, failing to dispose of data no longer needed for any legitimate business purpose, maintaining the data on an unsecured database in an unencrypted format, failing to adequately monitor activity on the servers containing Plaintiff's and the Class's information, and failing to adequately segment the sensitive data from other parts of Defendant's servers and networks.

252. Similarly, Defendant deployed knowingly unreasonable data security measures that defied expert recommendations, industry standards, and statutory requirements for reasonable data security.

253. Defendant's failure to comply with basic data security necessary to protect any stored data, much less the significant and highly private Personal Information Defendant stored, constitutes immoral, unethical, oppressive, and unscrupulous conduct that caused substantial harm to Plaintiff and the Class. That is especially true because, despite failing to reasonably protect Plaintiff's and the Class's highly sensitive and private Personal Information, Defendant gained significant profit from that information. Indeed, a significant part of Defendant's revenue was the use, analysis, and sale of data related to Plaintiff's Personal Information. While Defendant profited off of Plaintiff's and the Class's data, they failed to take the necessary measures to protect it, leaving Plaintiff and the Class at significant and foreseeable risk of harm.

254. Defendant violated the MDTPA by acting unfairly, unlawfully, and unscrupulously. Specifically, Defendant violated the MDTPA by developing the server subject to the breach, including collecting and aggregating Plaintiff's and the Class's Personal Information and putting in place knowingly unreasonable data security to protect that Personal Information. Defendant failed to follow its own policies, which required it to put in place certain measures to protect policyholders' Personal Information. Furthermore, Defendant's systems lacked other reasonable data security measures, as demonstrated by the cybercriminals' ability to move laterally within the system.

255. As a result of those unlawful and unfair business practices, Plaintiff and the Class's highly sensitive Personal Information was put at foreseeable risk of unauthorized access, theft, and acquisition. That risk materialized with the Data Breach, where hackers obtained and successfully exfiltrated the Personal Information of Plaintiff and the Class.

Subsequently, the stolen information was posted on the dark web, exposing their private and personal information and putting patients at a substantial risk of misuse of their data.

256. As a direct and proximate result of Defendant's inadequate security and the resulting Data Breach, Plaintiff suffered significant injuries, including, but not limited to: (1) loss of privacy; (2) misappropriation of their identity, name and likeness; (3) fraud and identity theft from the misuse of their stolen Personal Information; (4) diminution in the value of their Personal Information due to the loss of security, confidentiality, and privacy; (5) lost value of their Personal Information; (6) emotional and mental distress and anguish resulting from the access, theft and posting of their Personal Information; (7) lost time, effort and expense responding to and preventing the threats and harm posed by the Data Breach; and (8) a continued substantial and imminent risk of the misuse of their Personal Information.

257. Plaintiff and the Class also remain at heightened risk of future injury because their information resides with Defendant and, further, because Defendant continues to gather new information on Plaintiff and the Class. Without the use of adequate data security, Plaintiff and the Class remain at a heightened and substantial risk that their Personal Information will be subject to another data breach.

258. Plaintiff and the Class seek all monetary and non-monetary relief allowed by law, including any: economic damages; damages for emotional and mental anguish; nominal damages; enhanced or treble damages available under the law; court costs; reasonable and necessary attorneys' fees; injunctive relief; and any other relief available by law and to which the court deems proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a. For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and their counsel as Class Counsel;

b. For a declaration of rights regarding the reasonable protection of Plaintiff's Personal Information that remains in Defendant's possession and maintenance;

c. 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' Personal Information;

d. 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 Personal Information compromised during the Data Breach;

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

f. Ordering Defendant to pay for not less than five years of credit monitoring services for Plaintiff and the Class;

g. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, 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

j. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

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

Dated: July 28, 2025

s/Daniel E. Gustafson

Daniel E. Gustafson (#202241)
Shashi K. Gowda (#401809)
Frances Mahoney-Mosedale (#402741)
GUSTAFSON GLUEK PLLC
120 South Sixth Street #2600
Minneapolis, MN 55402
Telephone: (612) 333-8844
dgustafson@gustafsongluek.com
sgowda@gustafsongluek.com
fmahoneymosedale@gustafsongluek.com

Jon Tostrud
Anthony Carter
TOSTRUD LAW GROUP, PC
1925 Century Park East, Suite 2100
Los Angeles, CA 90067
Telephone: (310) 278-2600
jtostrud@tostrudlaw.com
acarter@tostrudlaw.com

Counsel for Plaintiff and the Proposed Class