UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF GEORGIA

ISMAEL PEREZ, individually and on behalf of all others similarly situated, Plaintiff, v. AFLAC INC., Defendant.	Case No. _____ CLASS ACTION JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Ismael Perez ("Plaintiff"), individually and on behalf of all others similarly situated (collectively, "Class members"), by and through his attorneys, brings this Class Action Complaint against Defendant Aflac Inc. ("Aflac" or "Defendant"), and complains and alleges upon personal knowledge as to himself and information and belief as to all other matters.

INTRODUCTION

1. Plaintiff brings this class action against Aflac for its failure to secure and safeguard the personally identifying information ("PII") and personal health information ("PHI") of Plaintiff and other current and former Aflac customers, including claims information, health information, social security numbers, and other personal information.

2. Aflac is an insurance company that provides supplemental insurance coverage.

3. On or about June 12, 2025, an unauthorized third party gained access to Aflac's network systems and accessed and copied files containing the PII/PHI of Aflac's customers, beneficiaries, employees, and agents (the "Data Breach").

4. Aflac owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Aflac breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect its customers' PII/PHI from unauthorized access and disclosure.

5. As a result of Aflac's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of himself and all persons whose PII/PHI was exposed as a result of the Data Breach, which occurred on or about June 12, 2025.

6. Plaintiff, on behalf of himself and all other Class members, asserts claims for negligence, negligence per se, breach of implied contract, and unjust enrichment, and seeks declaratory relief, injunctive relief, monetary damages,

statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

PARTIES

Plaintiff Ismael Perez

7. Plaintiff Ismael Perez is a resident and citizen of McAllen, Texas.

8. Plaintiff is a policyholder of Aflac. As a condition of obtaining insurance services from Aflac, Aflac required Plaintiff to provide it with his PII/PHI.

9. Plaintiff believed Aflac had implemented and maintained reasonable security and practices to protect his PII/PHI. With this belief in mind, Plaintiff provided his PII/PHI to Aflac in connection with obtaining insurance services from Aflac.

10. At all relevant times Aflac stored and maintained Plaintiff's PII/PHI on its network systems, including the systems accessed in the Data Breach.

11. Had Plaintiff known that Aflac does not adequately protect the PII/PHI in its possession, he would not have obtained insurance services from Aflac or agreed to entrust it with his PII/PHI.

12. Plaintiff received a notice email dated June 20, 2025 from Aflac notifying him that his PII/PHI was affected in the Data Breach.

13. As a result of Data Breach, Plaintiff has experienced upsticks in spam calls, SMS and emails and also there was an influx in fraud alerts.

14. As a direct result of the Data Breach, Plaintiff has suffered injury and damages including, *inter alia*, a substantially increased and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII/PHI; deprivation of the value of his PII/PHI; lost time and money mitigating the effects of the Data Breach; and overpayment for services that did not include adequate data security.

Defendant Aflac Inc.

15. Defendant Aflac Inc. is a Georgia corporation with its principal place of business located at 1932 Wynnton Rd, Columbus, GA 31999. It may be served through its registered agent: Audrey Boone Tillman, 1932 Wynnton Rd, Columbus, GA 31999.

JURISDICTION AND VENUE

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

17. This Court has general personal jurisdiction over Defendant Aflac Inc. because it is incorporated under the laws of this State and maintains its principal place of business in this District.

18. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

Overview of Aflac

19. Aflac is one of the largest insurance companies in the United States and provides supplemental insurance policies.[1]

20. In the regular course of its business, Aflac collects and maintains the PII/PHI of its current and former customers.[2] Aflac required Plaintiff and Class members to provide it with their PII/PHI as a condition of providing them with insurance services.

21. Aflac maintains a privacy notice (the "Privacy Notice") explaining how it uses and shares its customers private information.[3] In the Privacy Notice, Aflac admits it needs to use and share its customers' PII/PHI to run its business.[4]

---

[1] Pavlo Gonchar, *US insurance giant Aflac says customers' personal data stolen during cyberattack*, TECHCRUNCH (June 23, 2025 7:50 AM), https://techcrunch.com/2025/06/23/us-insurance-giant-aflac-says-customers-personal-data-stolen-during-cyberattack/.
[2] *Aflac Incorporated Discloses Cybersecurity Incident*, AFLAC (June 20, 2025), https://newsroom.aflac.com/2025-06-20-Aflac-Incorporated-Discloses-Cybersecurity-Incident (last accessed July 1, 2025).
[3] *See What Does Aflac Do With Your Personal Information?*, AFLAC (April 2025), https://www.aflac.com/docs/about-aflac/hipaa-glba-2017/glba-all-other-states-and-puerto-rico-english.pdf (last accessed July 1, 2025).
[4] *See id.*

22. In the Privacy Notice, Aflac promises it safeguards customers' PII/PHI by various means, including by "maintaining administrative, technical, and physical safeguards that comply with Federal and State laws" and include "computer safeguards;" limiting employee access to PII/PHI, and "providing privacy training and awareness to all employees."[5]

23. Aflac further promises customers' PII/PHI "shall be collected, used, and stored in accordance with applicable federal privacy laws" and state law.[6]

24. Aflac also maintains a Notice of Privacy Practices for protected health information (the "HIPAA Notice").[7] The HIPAA Notice "describes how Aflac may use and disclose Protected Health Information to carry out payment and health care operations, and for other purposes that are permitted or required by law."[8]

25. Aflac admits it is required to protect PII/PHI under HIPAA and other applicable laws.[9]

26. Aflac promises that it will not use or disclose its customers' PII/PHI other than the ways described in the HIPAA Notice without obtaining a customer's written consent.[10]

---

[5] *Id.*
[6] *Id.*
[7] *Notice of Privacy Practices – Protected Health Information*, AFLAC (Jan. 3, 2020), https://www.aflac.com/docs/about-aflac/hipaa-glba-2017/hipaa-all-states-and-puerto-rico-english.pdf (last accessed July 1, 2025).
[8] *Id.*
[9] *Id.*
[10] *Id.*

27. Aflac also promises it will inform its customers if there is a breach of their unsecured PII/PHI.[11]

28. Aflac maintains a privacy policy (the "Privacy Policy") that describes it collection and use of PII/PHI.[12]

29. Aflac states in the Privacy Policy it only retains PII/PHI for as long as necessary to achieve the purposes for which it obtained the information and to comply with legal obligations.[13]

30. Aflac promises it maintains "technical, physical, and administrative security measures designed to protect the security of your personal information against loss, misuse, unauthorized access, disclosure, or alteration."[14] Aflac specifies these measures include "firewalls, data encryption, physical access controls to our data centers and information access authorization controls."[15]

31. On its website, Aflac promises it "is fully committed to the security and protection of our customer's data."[16] Aflac warns customers to be wary of social engineering and that it can lead to identity theft.[17]

---

[11] *Id.*
[12] *Privacy Policy*, AFLAC (Jan. 1, 2023), https://www.aflac.com/privacy-center/privacy-policy.aspx#uses-retention (last visited July 1, 2025).
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Fraud & Security*, AFLAC, https://www.aflac.com/privacy-center/fraud-and-security.aspx (last accessed July 1, 2025).
[17] *Id.*

32. Aflac additionally promises it "maintain[s] physical, electronic and procedural safeguards that comply with applicable legal standards to secure such information from unauthorized access and use, accidental or unlawful alteration and destruction, and other unlawful or unauthorized forms of Processing."[18] It further promises its "Global Security team continuously evaluates and enhances how we protect our information using industry best practices."[19]

33. Aflac maintains a "Trust Center" that details its security measures.[20] Aflac represents to customers that its "commitment to data privacy and security is embedded in every part of our business."[21] Aflac represents it trains employees to recognize and avoid phishing scams.[22]

34. Plaintiff and Class members entrusted Aflac with their PII/PHI in exchange for insurance services.

The Data Breach

35. On or about June 12, 2025, Aflac identified suspicious activity on its network systems.[23] Aflac admits an "unauthorized party used social engineering tactics to gain access to our network" and accessed files containing the PII/PHI of Plaintiff and Class members, including "claims information, health information,

[18] *Id.*
[19] *Id.*
[20] *Trust Center*, AFLAC, https://cybertrust.aflac.com/ (last accessed July 1, 2025).
[21] *Id.*
[22] *Id.*
[23] *Aflac Incorporated Discloses Cybersecurity Incident*, *supra* note 2.

social security numbers, and/or other personal information, related to customers, beneficiaries, employees, agents, and other individuals."[24] Aflac further admits the Data Breach was caused by "a sophisticated cybercrime group."[25]

36. Defendant's failure to promptly notify Plaintiff and Class members that their PII/PHI was accessed and stolen virtually ensured that the unauthorized third parties who exploited those security lapses could monetize, misuse, or disseminate that PII/PHI before Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and Class members will suffer indefinitely from the substantial and concrete risk that their identities will be (or already have been) stolen and misappropriated.

Aflac Knew that Criminals Target PII/PHI

37. At all relevant times, Aflac knew, or should have known, that the PII/PHI that it collected, stored, and maintained was a target for malicious actors. Despite such knowledge, Aflac failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiff's and Class members' PII/PHI from cyberattacks that it should have anticipated and guarded against.

[24] *Id.*
[25] *Id.*

38. It is well known among companies that store sensitive personally identifying information that such information—such as the PII/PHI stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers . . . . Many of them were caused by flaws in . . . systems either online or in stores."[26]

39. Cyber criminals seek out PHI at a greater rate than other sources of personal information. In a 2025 report, Kroll found that "the healthcare industry was the most breached" in 2024.[27] The company found that 23% of the breaches that it handled responses for were from the healthcare industry, up from 18% in 2023.[28]

40. PII/PHI is a valuable property right.[29] The value of PII/PHI 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

[26] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUS. INSIDER (Nov. 19, 2019, 8:05 AM), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.
[27] *Data Breach Outlook*, KROLL, https://www.kroll.com/en/insights/publications/cyber/data-breach-outlook-2025 (last accessed July 1, 2025).
[28] *See id*.
[29] *See* Marc van Lieshout, *The Value of Personal Data*, 457 Int'l Fed'n for Info. Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible . . ."), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data.
[30] *See* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (April 28, 2014), http://www.medscape.com/viewarticle/824192.

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 PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

41. As a result of the real and significant value of these data, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security numbers, PII/PHI, and other sensitive information directly on various internet websites making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated with other such data and become more valuable to thieves and more damaging to victims.

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

[32] IAB Data Center of Excellence, *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 ADVERT. BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

42. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[33] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[34]

43. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, Social Security numbers, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[35] According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[36]

44. Criminals can use stolen PII/PHI to extort a financial payment by "leveraging details specific to a disease or terminal illness."[37] Quoting Carbon Black's Chief Cybersecurity Officer, one recent article explained: "Traditional criminals understand the power of coercion and extortion . . . By having healthcare

[33] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAG. (Oct. 20, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (quoting Tom Kellermann, Chief Cybersecurity Officer, Carbon Black, stating "Health information is a treasure trove for criminals.").
[34] *Id.*
[35] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices-in-the-online-black-market.
[36] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
[37] Steager, *supra* note 33.

information—specifically, regarding a sexually transmitted disease or terminal illness—that information can be used to extort or coerce someone to do what you want them to do."[38]

45. Consumers place a high value on the privacy of their data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[39]

46. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII/PHI has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

[38] *Id.*

[39] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFO. SYS. RSCH. 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

47. Theft of PII/PHI can have serious consequences for the victim. The FTC warns consumers that identity thieves use PII/PHI to receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.[40] [41]

48. Experian, one of the largest credit reporting companies in the world, warns consumers that "[i]dentity thieves can profit off your personal information" by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.[42]

49. Identity theft is not an easy problem to solve. In a survey, the Identity Theft Resource Center found that almost 20% of victims of identity misuse needed more than a month to resolve issues stemming from identity theft.[43]

---

[40] *See* Federal Trade Commission, *What to Know About Identity Theft*, FTC CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-identity-theft (last accessed July 1, 2025).

[41] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 12 C.F.R. § 1022.3(h). 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." 12 C.F.R. § 1022.3(g).

[42] *See* Louis DeNicola, *What Can Identity Thieves Do with Your Personal 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/.

[43] Identity Theft Resource Center, *2023 Consumer Aftermath Report*, IDENTITY THEFT RES. CTR. (2023), https://www.idtheftcenter.org/publication/2023-consumer-impact-report/ (last accessed July 1, 2025).

50. 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."[44] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[45] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use PII/PHI "to see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care." [46] The FTC also warns, "If the thief's health information is mixed with yours it could affect the medical care you're able to get or the health insurance benefits you're able to use."[47]

51. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

a. Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.

---

[44] Pam Dixon & John Emerson, *The Geography of Medical Identity Theft*, WORLD PRIV. F. (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.
[45] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk . . .*, *supra* note 36.
[46] *See* Federal Trade Commission, *What to Know About Medical Identity Theft*, FTC CONSUMER INFO., https://www.consumer.ftc.gov/articles/what-know-about-medical-identity-theft (last accessed July 1, 2025).
[47] *Id*.

b. Significant bills for medical goods and services neither sought nor received.

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

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

e. 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.

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

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

h. Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own. [48]

52. There may also be time lags 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 consumers to discover their

[48] *See* Dixon & Emerson, *supra* note 44.

identity has been stolen and used, but it takes some individuals up to three years to learn that information.[49]

53. It is within this context that Plaintiff and all other Class members must now live with the knowledge that their PII/PHI is forever in cyberspace and was taken by someone intending to use that information for any number of improper purposes and scams, including making the information available for sale on the black-market.

Damages Sustained by Plaintiff and Class Members

54. Plaintiff and Class members have suffered and will continue to suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendant's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data

[49] 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.

Breach; and (vii) overpayment for services that were received without adequate data security.

CLASS ALLEGATIONS

55. This action is brought and may be properly maintained as a class action pursuant to Fed. R. Civ. P. 23.

56. Plaintiff brings this action on behalf of himself and all members of the following Class of similarly situated persons:

> All persons whose personally identifiable information and personal health information was accessed by and disclosed in the Data Breach to unauthorized persons, including all who were sent a notice of the Data Breach.

57. Excluded from the Class are Aflac Inc., and its affiliates, parents, subsidiaries, officers, agents, and directors, as well as the judge(s) presiding over this matter and the clerks of said judge.

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

59. The members in the Class are so numerous that joinder of each of the Class members in a single proceeding would be impracticable. While Aflac has not yet released the total number of individuals affected in the Data Breach, upon

information and belief Plaintiff believes the Class likely contains thousands of members.

60. Common questions of law and fact exist as to all Class members and predominate over any potential questions affecting only individual Class members. Such common questions of law or fact include, *inter alia*:

a. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class members' PII/PHI from unauthorized access and disclosure;

b. Whether Defendant had a duty not to disclose the PII/PHI of Plaintiff and Class members to unauthorized third parties;

c. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII/PHI;

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

e. Whether Defendant breached its duties to protect Plaintiff's and Class members' PII/PHI; and

f. Whether Plaintiff and Class members are entitled to damages and the measure of such damages and relief.

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

62. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had his PII/PHI compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

63. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representative of the Class in that he has no interests adverse to, or that conflict with, the Class he seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

64. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class members to individually seek redress from Defendant's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the

delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE

65. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

66. Aflac owed a duty to Plaintiff and all other Class members to exercise reasonable care in safeguarding and protecting the PII/PHI in its possession, custody, or control.

67. Aflac knew, or should have known, the risks of collecting, sharing, and storing Plaintiff's and Class members' PII/PHI, and the importance of maintaining secure systems. Aflac knew, or should have known, of the many data breaches that targeted companies storing PII/PHI in recent years.

68. Given the nature of Aflac's business, the sensitivity and value of the PII/PHI it collects, stores, and maintains, and the resources at its disposal, Aflac should have identified the vulnerabilities in its systems and prevented the Data Breach from occurring.

69. Aflac breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing

to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

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

71. But for Aflac's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

72. As a result of Aflac's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class members have suffered and will continue to suffer injury including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery

from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendant's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT II
NEGLIGENCE PER SE

73. Plaintiff realleges and incorporates by reference preceding paragraphs 1-64 as if fully set forth herein.

74. Aflac's duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA 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 (collectively, "HIPAA Privacy and Security Rules").

75. Defendant's duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or

practice by business, such as Aflac, of failing to employ reasonable measures to protect and secure PII/PHI.

76. Aflac violated HIPAA Privacy and Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and other Class members' PII/PHI, and by not complying with applicable industry standards. Aflac's conduct was particularly unreasonable given the nature and amount of PII/PHI it obtains and shares, and the foreseeable consequences of a data breach involving PII/PHI including, specifically, the substantial damages that would result to Plaintiff and the other Class members.

77. Plaintiff and Class members are within the class of persons that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to protect.

78. The harm occurring as a result of the Data Breach is the type of harm that HIPAA Privacy and Security Rules and Section 5 of the FTCA were intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair practices or deceptive practices, caused the same type of harm that has been suffered by Plaintiff and Class members as a result of the Data Breach.

79. Aflac knew or should have known the risks of collecting, storing, and sharing Plaintiff's and all other Class members' PII/PHI. Aflac knew or should have known of the many data breaches that targeted insurance companies that collect and share PII/PHI in recent years.

80. Given the nature of Aflac's business, the sensitivity and value of the PII/PHI it collects and maintains, and the resources at its disposal, Aflac should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring.

81. Aflac breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

82. It was reasonably foreseeable to Aflac that its failure to exercise reasonable care in safeguarding, protecting, and sharing Plaintiff's and Class members' PII/PHI by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the

unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

83. But for Aflac's negligent conduct or breach of the above-described duties owed to Plaintiff and Class members, their PII/PHI would not have been compromised.

84. As a result of Aflac's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered and will continue to suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendant's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security.

COUNT III
BREACH OF IMPLIED CONTRACT

85. Plaintiff realleges and incorporates by reference preceding paragraphs 1-64 as if fully set forth herein.

86. In connection with receiving insurance services, Plaintiff and all other Class members entered into implied contracts with Aflac.

87. Pursuant to these implied contracts, Plaintiff and Class members paid money to Aflac and provided Aflac with their PII/PHI. In exchange, Aflac agreed to, among other things, and Plaintiff and Class members understood that Aflac would: (1) provide insurance services to Plaintiff and Class members; (2) collect, maintain, and utilize Plaintiff's and Class members' PII/PHI to, among other things, facilitate the provision of insurance services to Plaintiff and Class members; (3) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; (4) protect Plaintiff's and Class members' PII/PHI in compliance with federal and state laws and regulations, industry standards, and Aflac's representations; and (5) maintain the confidentiality of Plaintiff's and Class members' PII/PHI and protect it from unauthorized access, disclosure, theft, and misuse.

88. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Aflac, on the other hand. Indeed, as set forth supra, Aflac recognized the importance of

data security and the privacy of its customers' PII/PHI in its Privacy Policy and HIPAA Notice. Had Plaintiff and Class members known that Aflac would not adequately protect its customers' PII/PHI, they would not have agreed to provide Aflac with their PII/PHI or received insurance services from Aflac.

89. Plaintiff and Class members performed their obligations under the implied contract when they provided Aflac with their PII/PHI and paid for insurance services from Aflac.

90. Aflac breached its obligations under its implied contracts with Plaintiff and Class members in failing to implement and maintain reasonable security measures to protect and secure their PII/PHI and in failing to implement and maintain reasonable security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner that complies with applicable laws, regulations, industry standards, and Aflac's representations.

91. Aflac's breach of its obligations of its implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

92. Plaintiff and all other Class members were damaged by Aflac's breach of implied contracts because: (i) they paid for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for

which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) overpayment for services that were received without adequate data security.

COUNT IV
UNJUST ENRICHMENT

93. Plaintiff realleges and incorporates by reference preceding paragraphs 1-64 as if fully set forth herein.

94. This claim is pleaded in the alternative to the breach of implied contract claim.

95. Plaintiff and Class members conferred a monetary benefit upon Aflac in the form of monies paid to Aflac for insurance services and through the provision of their PII/PHI, which was necessary for Aflac to conduct its business. Plaintiff and Class members did so with an implicit understanding that Aflac would use some of these payments to protect the PII/PHI it collects, stores, and uses to provide insurance services.

96. Aflac accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class members. Aflac also benefitted from the receipt of Plaintiff's and Class members' PII/PHI, as this was used to facilitate its business operations.

97. As a result of Aflac's conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that they paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

98. Aflac should not be permitted to retain the money belonging to Plaintiff and Class members because Aflac failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

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

100. Aflac should be compelled to provide for the benefit of Plaintiff and Class members all unlawful proceeds received by it as a result of the conduct and Data Breach alleged herein.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the Class, respectfully requests that the Court enter judgment in his favor and against Defendant as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class Representative, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of himself and the Class, seeks appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and implementing best data security practices to safeguard PII/PHI and to provide or extend credit monitoring services and similar services to protect against all types of identity theft and medical identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable under law;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: July 3, 2025