UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS

DENIA ELIZARRARAS, individually and on behalf of all others similarly situated, Plaintiff, v. **GLOBE LIFE, INC.,** Defendant.	Case No. **COMPLAINT AND DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiff, Denia Elizarraras ("Plaintiff"), brings this Class Action Complaint ("Complaint") against Defendant, Globe Life Inc. ("Globe Life" or "Defendant"), as an individual and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions, and upon information and belief and her counsel's investigation as to all other matters, as follows:

INTRODUCTION

1. Plaintiff seeks injunctive and declaratory relief arising from Defendant's failure to safeguard the names, email addresses, phone numbers, postal addresses, and Social Security numbers, ("Personally Identifiable Information")[1] and health data and insurance policy information ("Protected Health Information") (together, "Private Information") of its Customers, which resulted in unauthorized access to its information systems in or around October 2024, and

[1] The Federal Trade Commission ("FTC") defines "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." 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendant, not every type of information included in that definition was compromised in the subject data breach.

the compromised and unauthorized disclosure of that Private Information, causing widespread injury and damages to Plaintiff and the proposed Class (defined below) members.

2. Defendant, Globe Life Inc. is an insurance company that offers life insurance policies with its principal place of business in McKinney, Texas[2].

3. As explained in detail herein, in or around October 2024, Globe Life detected unusual activity in its computer systems and ultimately determined that an unauthorized third party accessed its network and obtained certain files from its systems in or around October 2024. ("Data Breach").[3]

4. As a result of the Data Breach, which Defendant failed to prevent, the Private Information of Defendant's Customers, including Plaintiff and the proposed Class Members, were stolen, including their names, email addresses, phone numbers, postal addresses, and Social Security numbers, health data and insurance policy information.[4]

5. Defendant's investigation concluded that the Private Information compromised in the Data Breach included Plaintiff's and other individuals' information (together, "Customers").

6. Defendant's failure to safeguard Customers' highly sensitive Private Information as exposed and unauthorizedly disclosed in the Data Breach violates its common law duty, Texas law, and Defendant's implied contract with its Customers to safeguard their Private Information.

7. Plaintiff and Class Members now face a lifetime risk of identity theft due to the nature of the information lost, which they cannot change, and which cannot be made private again.

8. Defendant's harmful conduct has injured Plaintiff and Class Members in multiple ways, including: (i) the lost or diminished value of their Private Information; (ii) costs associated

[2] https://e806.globelifeinsurance.com/about#historyofglobe (last visited Feb. 28, 2025).
[3] https://therecord.media/globe-life-updated-sec-filing-hackers-extortion-data-breach (last visited Feb. 28, 2025).
[4] *Id.*

with the prevention, detection, and recovery from identity theft, tax fraud, and other unauthorized use of their data; (iii) lost opportunity costs to mitigate the Data Breach's consequences, including lost time; and (iv) emotional distress associated with the loss of control over their highly sensitive Private Information.

9. Defendant's failure to protect Customers' Private Information has harmed and will continue to harm Defendant's Customers, causing Plaintiff to seek relief on a Class wide basis.

10. On behalf of herself and the Class preliminarily defined below, Plaintiff brings causes of action against Defendant for negligence, negligence *per se*, breach of fiduciary duty, and breach of implied contract, resulting from Defendant's failure to adequately protect their highly sensitive Private Information.

PARTIES

11. Plaintiff is, and at all times mentioned herein was, an individual resident and citizen of the State of California.

12. Plaintiff is a customer of Defendant. As a condition of being a customer, Defendant required Plaintiff to provide them with her Private Information.

13. Defendant Globe Life Inc. is a Delaware corporation with its headquarters and principal place of business in McKinney, Texas.

JURISDICTION AND VENUE

14. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1332(d)(2), because the matter in controversy exceeds $5,000,000, exclusive of interest and costs, and is a class action in which at least one member of the class is a citizen of a different State than Defendant, including Plaintiff. The number of members of the proposed Classes is over

850,000 customers[5]. 28 U.S.C. § 1332(d)(5)(B).

15. This Court has personal jurisdiction over the Defendant because it regularly conducts and/or solicits business in, engages in other persistent courses of conduct in, and/or derives substantial revenue from products and/or services provided to persons in this District.

16. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Defendant does business in this District and because a substantial part of the events or omissions giving rise to the claims occurred in this District.

FACTUAL BACKGROUND

Defendant Globe Life Inc's. Business

17. Globe Life Inc. is an insurance company that offers life insurance policies to consumers.[6]

18. Plaintiff and Class Members are current or former Customers who provided their Private Information to Defendant.

19. To receive insurance policies, Customers, including Plaintiff and Class Members, were required to provide sensitive and confidential Private Information, including their names, dates of birth, health records, insurance information, and other sensitive information, that would be held by Globe Life in its computer systems.

20. The information held by Globe Life at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class Members.

21. Upon information and belief, Globe Life made promises and representations to its Customers that the Private Information collected would be kept safe and confidential, the privacy

[5] https://therecord.media/globe-life-updated-sec-filing-hackers-extortion-data-breach (last visited Feb. 28, 2025).
[6] https://e806.globelifeinsurance.com/about(last visited Feb. 28, 2025).

of that information would be maintained, and Globe Life would delete any sensitive information after it was no longer required to maintain it.

22. Plaintiff and Class Members provided their Private 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.

23. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

24. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep Customers' Private Information safe and confidential.

25. Defendant had obligations under the FTC Act, HIPAA, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

26. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Private Information, Defendant could not provide its services.

27. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private

Information from disclosure.

The Data Breach

28. On or around June 13, 2024, Globe Life discovered an unauthorized actor gained access to and compromised its IT network "Data Breach".

29. In or around October 2024, Defendant filed a notice with the U.S. Securities and Exchange Commission (SEC), stating it experienced a Data Breach in which the confidential information of over 5,000 consumers was exposed.[7]

30. On January 31, 2025, Defendant filed another notice with the SEC, stating that after further investigation, the Data Breach affected over 850,000 individuals.[8]

31. To be clear, there are numerous issues with the Globe Life Data Breach, but the deficiencies in the way Globe Life has handled the Breach exacerbate the circumstances for victims of the Data Breach: (1.) At no point has Globe Life notified its Customers about the Data Breach and the exposure of their confidential information; (2.) Globe Life waited ***four*** months to notify the SEC of the Data Breach; (3.) In its notice to the SEC, Globe Life fails to state whether it was able to contain or end the cybersecurity threat, leaving victims to fear whether the Private Information that Globe Life continues to maintain is secure; and (4) Globe Life fails to state how the breach itself occurred. All of this information is vital to victims of a data breach, let alone a data breach of this magnitude due to the sensitivity and wide array of information compromised in this specific breach.

32. Furthermore, Defendant's refusal to notify Plaintiff and Class Members of the Data Breach is in direct violation of Defendant's responsibilities under the data breach notification

[7] https://www.jdsupra.com/legalnews/data-breach-at-globe-life-s-american-7377612/ (last visited Feb. 28, 2025).
[8] *Id.*

statute in Texas. See Texas Identity Theft Enforcement And Protection Act which requires that the disclosure notification must be made "without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred".[9]

33. To this day, Defendant has still not mailed out any notices to its customers, nor have they posted a notice or any information regarding the Data Breach on their website.

34. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class Members, such as encrypting the information or deleting it when it is no longer needed, causing the exposure of Private Information.

35. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted Private Information of Plaintiff and Class Members, including names, email addresses, phone numbers, postal addresses, and Social Security numbers, health data and insurance policy information. Plaintiff's and Class Members' Private Information was accessed and stolen in the Data Breach.

36. Plaintiff further believes her Private Information, and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

The Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' Private Information.

37. As a condition of receiving insurance policies from Globe Life, Plaintiff and Class Members were required to give their sensitive and confidential Private Information to Globe Life.

38. Globe Life retains and stores this information and derives a substantial economic

[9] Texas requires the notification to be made within 60 days of discovery of the breach, and "unreasonable delay" is anything that exceeds that. Defendant failed to meet this deadline by over 100 days and counting, as consumers have still not received notification of the Data Breach.

benefit from the Private Information that it collects. But for the collection of Plaintiff's and Class Members' Private Information, Globe Life would be unable to sell its insurance policies.

39. By obtaining, collecting, and storing the Private Information of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the Private Information from disclosure.

40. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

41. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiff and Class Members.

42. Upon information and belief, Defendant made promises to Plaintiff and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information, including through its privacy policies.[10]

43. Defendant's negligence in safeguarding the Private Information of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

Defendant Knew or Should Have Known of the Risk of a Cyber Attack Because Healthcare Entities in Possession of Private Information Are Particularly Suspectable to Cyber Attacks

44. Data thieves regularly target entities in the healthcare industry like Defendant due

[10] See https://e806.globelifeinsurance.com/privacy ("Globe Life Inc. companies are committed to ensuring that our practices regarding the privacy of the personal information we collect from you align with industry norms, adhere to contractual obligations, and comply with all applicable laws") (last visited Feb. 28, 2025).

to the highly sensitive information that they maintain. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

45. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities like Defendant that collect and store Private Information and other sensitive information, preceding the date of the Data Breach.

46. In light of recent high profile data breaches at other industry-leading companies, including, *e.g.*, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that the Private Information that it collected and maintained would be targeted by cybercriminals.

47. For example, of the 1,862 recorded data breaches in 2021, 330 of them, or 17.7%, were in the medical or healthcare industry.[11]

48. The 330 breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[12]

49. Entities in custody of PHI and/or medical information reported the largest number of data breaches among all measured sectors in 2022, with the highest rate of exposure per breach.[13] Indeed, when compromised, healthcare related data is among the most sensitive and

[11] 2021 Data Breach Annual Report (ITRC, Jan. 2022), https://notified.idtheftcenter.org/s/, at 6.
[12] *Id*.
[13] *See* Identity Theft Resource Center, *2022 Annual Data Breach Report*, https://GlobeLife.idtheftcenter.org/publication/2022-data-breach-report/ (last visited Feb. 28, 2025).

personally consequential. A report focusing on healthcare breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and that victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.[14] Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. 40 percent of the patients were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals, and detrimentally impact the economy as a whole.[15]

50. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and Class Members from being compromised.

51. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to thousands of individuals' detailed Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

52. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

53. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen fraudulent use of that information and damage to victims may continue for years.

54. As a healthcare entity in possession of its Customers' Private Information,

[14] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), https://Globe Life.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited Feb. 28, 2025).
[15] *See id.*

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

Defendant Fails to Comply with FTC Guidelines

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

56. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[16]

57. 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.[17]

58. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require

[16] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (2016), https://Globe Life.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Feb. 28, 2025).
[17] *Id.*

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.

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

60. These FTC enforcement actions include actions against healthcare entities, like Defendant. *See, e.g., In the Matter of LabMD, Inc., a corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

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

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

63. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Customers' Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15

U.S.C.

§ 45.

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

Defendant Fails to Comply with HIPAA Guidelines

65. Defendant is a covered businesses under HIPAA (45 C.F.R. § 160.102) and is required to comply with 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.

66. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[18] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

67. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

68. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

[18] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

69. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

70. "Electronic protected health information" is "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

71. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

72. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

73. HIPAA and HITECH also obligate Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic PHI that are reasonably anticipated but not permitted by the privacy

rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

74. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

75. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of PHI in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

76. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[19] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI." US Department of Health & Human Services, Guidance on Risk Analysis.[20]

Defendant Owed Plaintiff and Class Members a Duty to Safeguard their Private Information

[19] https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited Feb. 28, 2025).

[20] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last visited Feb. 28, 2025).

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

78. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

79. Defendant owed a duty to Plaintiff and Class Members to implement processes that would detect a compromise of Private Information in a timely manner.

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

81. Defendant owed a duty to Plaintiff and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

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

The Data Breach Increases Plaintiff's and Class Members' Risk of Identity Theft

83. The unencrypted Private Information of Plaintiff and Class Members will end up (if it has not already ended up) for sale on the dark web, as that is the *modus operandi* of hackers.

84. Unencrypted Private Information may also fall into the hands of companies that

will use the detailed Private Information for targeted marketing without the approval of Plaintiff and Class Members.

85. Simply put, unauthorized individuals can easily access the Private Information of Plaintiff and Class Members because of the Data Breach.

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

87. Plaintiff's and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiff and Class Members and to profit from their misfortune.

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

88. As a result of the recognized risk of identity theft, when a data breach occurs and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm.

89. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must monitor their financial accounts for many years to mitigate the risk of identity theft.

90. Plaintiff and Class Members have spent, and will spend additional time in the

future, on a variety of prudent actions, such as changing passwords and resecuring their own computer systems.

91. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[21]

92. Plaintiff's mitigation efforts are also consistent with the steps the FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[22]

93. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

Diminution of Value of Private Information

94. Private Information is valuable property.[23] Its value is axiomatic, considering the

[21] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf (last visited Feb. 28, 2025).

[22] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited Feb. 28, 2025).

[23] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," at 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Feb. 28, 2025) ("GAO Report").

value of Big Data in corporate America and that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk-to-reward analysis illustrates, beyond doubt, that Private Information has considerable market value.

95. The Private Information stolen in the Data Breach is significantly more valuable than the loss of, say, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information stolen in the Data Breach is difficult, if not impossible, to change.

96. This kind of data, as one would expect, demands a much higher price on the dark web. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[24]

97. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[25]

98. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[26] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data

[24] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hackpersonal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Feb. 28, 2025).

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

[26] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Feb. 28, 2025).

broker who in turn aggregates the information and provides it to marketers or app developers.[27,28] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50 a year.[29]

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

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

101. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

102. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to millions of individuals' detailed Private Information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

103. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private

[27] https://latimes.com/business/story/2019-11-05/column-data-brokers (last visited Feb. 28, 2025).
[28] https://datacoup.com/ (last visited Feb. 28, 2025).
[29] https://www.thepennyhoarder.com/make-money/nielsen-panel/#:~:text=Sign%20up%20to%20join%20the,software%20installed%20on%20your%20computer (last visited Feb. 28, 2025).

Information of Plaintiff and Class Members.

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

104. Given the type of targeted attack in this case, the sophisticated criminal activity, the volume of data compromised in this Data Breach, and the sensitive type of Private Information involved in this Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

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

106. Consequently, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

107. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft resulting from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear, but for Defendant's failure to safeguard their Private Information.

Loss of the Benefit of the Bargain

108. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members

of the benefit of their bargain. When agreeing to pay Defendant for insurance policies, Plaintiff and other reasonable Customers understood and expected that they were, in part, paying for the services and necessary data security to protect the Private Information when, in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff's Experience

109. Plaintiff purchased an insurance policy from Globe Life. To receive the policy, she was required to provide her Private Information to Globe Life.

110. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff's Private Information in its system.

111. Plaintiff is very careful about sharing her sensitive Private Information. Plaintiff stores any documents containing her Private Information in a safe and secure location. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source.

112. Plaintiff learned of the data breach online. According to the news report, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties. The Private Information comprised some combination of her name, email address, phone number, postal address, and Social Security number, health data and insurance policy information.

113. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including checking her bills and accounts to make sure they were correct. Plaintiff has spent significant time dealing with the Data Breach, valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation.

This time has been lost forever and cannot be recaptured.

114. As a result of the Data Breach, Plaintiff fears for her personal financial security and uncertainty over what medical information was revealed in the Data Breach. She is experiencing feelings of anxiety, sleep disruption, stress, and fear because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

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

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

117. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

118. Plaintiff brings this suit on behalf of herself and a Class of similarly situated individuals on behalf of the following Classes:

> All individuals in the United States who purchased life insurance policies from Globe Life and whose Private Information was accessed and/or acquired by an unauthorized party in the Data Breach. (the "Class").
>
> All individuals in the state of California who purchased life insurance policies from Globe Life and whose Private Information was accessed and/or acquired by an unauthorized party in the Data Breach. (the "California Subclass").

119. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded

from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

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

121. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. The Class is believed to include over 850,000 individuals.[30] The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

122. **Commonality.** Common questions of law and fact exist as to all Class Members and predominate over any questions affecting solely individual Class Members. Among the questions of law and fact common to the Classes that predominate over questions which may affect individual Class Members, are the following:

a. Whether and to what extent Defendant has a duty to protect the Private Information of Plaintiff and Class Members;

b. Whether Defendant has respective duties not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant has respective duties not to use the Private Information of Plaintiff and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;

e. Whether Defendant failed to implement and maintain reasonable security

[30] https://www.jdsupra.com/legalnews/data-breach-at-globe-life-s-american-7377612/ (last visited Feb. 28, 2025)

procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

f. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

g. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

123. **Typicality.** The claims of the Plaintiff, who is the representative of the Classes herein, are typical of the claims of the proposed Classes, in that the claims of all members of the proposed Classes, including the Plaintiff, depend on a showing of the acts of Defendants giving rise to the right of Plaintiff to the relief sought herein. There is no conflict between the individually named Plaintiff and the other members of the proposed Classes with respect to this action, or with respect to the claims for relief set forth herein.

124. **Adequacy of Representation.** Plaintiff is an adequate representative of the Classes because Plaintiff's interests do not conflict with the interests of the other Class Members whom he seeks to represent. Plaintiff has retained counsel competent and experienced in complex class action litigation, including successfully litigating class action cases similar to this one, where insurers breached contracts with insureds. The interests of the Classse will be fairly and adequately protected by Plaintiff and her counsel.

125. **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. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high

and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

CAUSES OF ACTION

COUNT I

Negligence

(On behalf of Plaintiff and the Class)

126. Plaintiff hereby repeats and realleges paragraphs 1 through 125 of this Complaint and incorporates them by reference herein.

127. Defendant requires its Customers, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of selling insurance policies.

128. Defendant gathered and stored the Private Information of Plaintiff and Class Members as part of its business of soliciting its services to its Customers, which solicitations and products affect commerce.

129. Plaintiff and Class Members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

130. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

131. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' Private Information

held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

132. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

133. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

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

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

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

137. Defendant breached its duties, thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, (a) failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information; (b) failing to adequately monitor the security of their networks and systems; and (c) allowing unauthorized access to Class Members' Private Information.

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

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

140. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed.

141. Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and Class Members, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

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

143. Plaintiff and Class Members had no ability to protect their Private Information that was in, and likely remains in, Defendant's possession.

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

145. Defendant's duty extended to protecting Plaintiff and Class Members from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

146. Defendant has admitted that the Private Information of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

147. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the Private Information of Plaintiff and Class Members would not have been compromised.

148. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiff and Class Members and the harm, or risk of imminent harm, suffered by Plaintiff and Class Members. The Private Information of Plaintiff and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

149. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy;

(ii) lost or diminished value of their Private Information; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

150. As a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

151. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

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

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

153. Plaintiff hereby repeats and realleges paragraphs 1 through 125 of this Complaint

and incorporates them by reference herein.

154. Pursuant to the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

155. Pursuant to HIPAA, 42 U.S.C. § 1302d *et seq.*, Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

156. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." *See* definition of encryption at 45 C.F.R. § 164.304.

157. Defendant breached its duties to Plaintiff and Class Members under the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

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

159. The injuries to Plaintiff and Class Members resulting from the Data Breach were directly and indirectly caused by Defendant's violation of the statutes described herein.

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

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

162. The injuries and harms suffered by Plaintiff and Class Members were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

COUNT III
Breach of Fiduciary Duty
(On behalf of Plaintiff and the Class)

163. Plaintiff hereby repeats and realleges paragraphs 1 through 125 of this Complaint and incorporates them by reference herein.

164. Plaintiff and the other Class Members gave Defendant their Private Information believing that Defendant would protect that information. Plaintiff and the other Class Members would not have provided Defendant with this information had they known it would not be adequately protected. Defendant's acceptance and storage of Plaintiff's and the other Class Members' Private Information created a fiduciary relationship between Defendant on the one hand, and Plaintiff and the other Class Members, on the other hand. In light of this relationship, Defendant must act primarily for the benefit of its Customers, which includes safeguarding and protecting Plaintiff's and the other Class Members' Private Information.

165. Due to the nature of the relationship between Defendant and Plaintiff and the other Class Members, Plaintiff and the other Class Members were entirely reliant upon Defendant to ensure that their Private Information was adequately protected. Plaintiff and the other Class Members had no way of verifying or influencing the nature and extent of Defendant's or their vendors' data security policies and practices, and Defendant was in an exclusive position to guard against the Data Breach.

166. Defendant has a fiduciary duty to act for the benefit of Plaintiff and the other Class Members upon matters within the scope of their relationship. It breached that duty by contracting with companies that failed to properly protect the integrity of the systems containing Plaintiff's and the other Class Members' Private Information, failing to comply with the data security guidelines set forth by HIPPA, and otherwise failing to safeguard Plaintiff's and the other Class Members' Private Information that they collected.

167. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and the other Class Members have suffered and will 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 Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their Private Information; (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 Private Information 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 Private Information compromised as a result of the Data breach; (vii) loss of potential value of their Private Information; (viii) overpayment for the services that were received without adequate data security.

COUNT IV
Breach of Implied Contract
(On behalf of Plaintiff and the Class)

168. Plaintiff hereby repeats and realleges paragraphs 1 through 125 of this Complaint and incorporates them by reference herein.

169. Defendant offered to provide insurance policies to its Customers, including Plaintiff and Class Members, in exchange for payment.

170. Defendant also required Plaintiff and the Class Members to provide their Private Information to receive insurance policies.

171. In turn, Defendant impliedly promised and represented to protect Plaintiff's and Class Members' Private Information through adequate data security measures, including through its privacy policies.

172. Plaintiff and the Class Members accepted Defendant's offer by providing Private Information to Defendant in exchange for receiving Defendant's services, and then by paying for and receiving the same.

173. Plaintiff and Class Members would not have paid for Defendant's services or entrusted their Private Information to Defendant but for the above-described agreement with Defendant.

174. Defendant materially breached its agreement(s) with Plaintiff and Class Members by failing to safeguard such Private Information, violating industry standards necessarily incorporated in the agreement.

175. Plaintiff and Class Members have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

176. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract along with its form.

177. Defendant's conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract.

178. The losses and damages Plaintiff and Class Members sustained as described herein were the direct and proximate result of Defendant's breach of the implied contracts with them, including breach of the implied covenant of good faith and fair dealing.

COUNT V
California Consumer Privacy Act
Cal. Civ. Code §§ 1798.100 *et seq.* ("CCPA")
(On Behalf of Plaintiff and the California Subclass)

179. Plaintiff hereby repeats and realleges paragraphs 1 through 125 of this Complaint and incorporates them by reference herein.

180. Defendant is a corporation organized or operated for the profit or financial benefit of its owners. Defendant collects consumers' Private Information (for the purposes of this section, "Private Information") as defined in the California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.140.

181. Defendant violated § 1798.150 of the CCPA by failing to prevent Plaintiff's and California Subclass Members' nonencrypted Private Information from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

182. Defendant has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff's and California Subclass Members' Private Information. As detailed herein, Defendant failed to do so.

183. As a direct and proximate result of Defendant's acts, Plaintiff's and California Subclass Members' Private Information, including names, email addresses, phone numbers, postal addresses, and Social Security numbers, health data and insurance policy information, was

subjected to unauthorized access and exfiltration, theft, or disclosure.

184. Plaintiff and California Subclass Members seek injunctive or other equitable relief to ensure Defendant hereinafter properly safeguards customer Private Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold customer Private Information, including Plaintiff's and California Subclass Members' Private Information. Plaintiff and California Subclass Members have an interest in ensuring that their Private Information is reasonably protected.

185. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant and third parties with similar inadequate security measures.

186. Plaintiff and California Subclass Members seek actual damages, as well as all monetary and non-monetary relief allowed by law, including actual financial losses; injunctive relief; and reasonable attorneys' fees and costs.

187. On March 3, 2025, counsel for Plaintiff provided written notice via certified mail to Defendant at its principal place of business of the intent to pursue claims under the CCPA and an opportunity for Defendant to cure. The domestic return receipt shows that Defendant received the letter. Plaintiff's written notice set forth the violations of Defendant's duty to implement and maintain reasonable security procedures and practices alleged in this Consolidated Class Action Complaint.

188. To date, Defendant has taken no action to remedy its misconduct or otherwise address the violations outlined in the written notice sent by Plaintiff's counsel.

189. Plaintiff and the California Subclass seek actual damages, as well as all monetary and non-monetary relief allowed by law, including statutory damages of up to $750 per customer

per incident, actual financial losses; injunctive relief; and reasonable attorneys' fees and costs. *See* Cal. Civil Code § 1798.150.

COUNT VI
California Consumer Records Act
Cal. Civ. Code §§ 1798.82 *et seq.* ("CCRA")
(On Behalf of Plaintiff and the California Subclass)

190. Plaintiff hereby repeats and realleges paragraphs 1 through 125 of this Complaint and incorporates them by reference herein.

191. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay. . . ."

192. The CCRA further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b).

193. The CCRA specifies certain requirements when entities subject to its purview are required to issue a security breach notification, including that such entities do not unreasonably delay such notifications.

194. Defendant unreasonably delayed—by more than one year—before sending notice of the breach to California Subclass Members.

195. As a result of Defendant's violation of the CCRA, Plaintiff and California Subclass Members were deprived of prompt notice of the Data Breach and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiff and California Subclass Members because their stolen information would have had less value to identity thieves.

196. As a result of Defendant's violation of the CCRA, Plaintiff and California Subclass Members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breach itself.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and Class Members, requests judgment against Defendant and that the Court grants the following:

A. For an order certifying the Class, as defined herein, and appointing Plaintiff and her Counsel to represent the Class;

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

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

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws.

iii. requiring Defendant to delete, destroy, and purge the Private Information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive information security program designed to protect the confidentiality and integrity of the Private Information of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the Private Information of Plaintiff and Class Members on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating

firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and security checks;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves; and

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

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

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury of all issues so triable.

Dated: March 3, 2025.

Respectfully submitted,

By: */s/Andrew Shamis*
Andrew J. Shamis
Leanna A. Loginov
SHAMIS & GENTILE, P.A.
14 NE 1st Avenue, Suite 705
Miami, FL 33132
Telephone: 305-479-2299
ashamis@shamisgentile.com
lloginov@shamisgentile.com

Jeff Ostrow
Ken Grunfeld*
KOPELOWITZ OSTROW, P.A.
One West Las Olas Blvd., Suite 500
Ft. Lauderdale, FL 33301
Tel: 954-525-4100
ostrow@kolawyers.com
grunfeld@kolawyers.com

Attorneys for Plaintiff and the Putative Class

**pro hac vice* forthcoming

JS 44 (Rev. 03/24)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

DENIA ELIZARRARAS, individually and on behalf of all others similarly situated,

(b) County of Residence of First Listed Plaintiff Orange County, CA
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Shamis & Gentile, P.A., 14 NE 1st Avenue, Suite 705, Miami, Florida 33132 - (305) 479-2299

DEFENDANTS

GLOBE LIFE, INC.

County of Residence of First Listed Defendant Collin County, TX
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☒ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)(2)

Brief description of cause:
Data Breach

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5,000,000

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE: March 3, 2025

SIGNATURE OF ATTORNEY OF RECORD: /s/ Andrew Shamis

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. Origin. Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related cases, if any. If there are related cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.