UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS
EASTERN DIVISION

ROBERT FRANCIS and JOHN GOODWIN, on behalf of themselves and all others similarly situated, Plaintiffs, v. **LIBERTY MUTUAL INSURANCE COMPANY**, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs, Robert Francis and John Goodwin ("Plaintiffs"), on behalf of themselves and all others similarly situated, state as follows for their class action complaint against Defendant, LIBERTY MUTUAL INSURANCE COMPANY ("Liberty Mutual" or "Defendant"):

INTRODUCTION

1. This class action arises from Defendant's failure to properly secure and safeguard Plaintiffs' and Class Members' sensitive personally identifiable information ("PII") and protected health information ("PHI" and collectively with PII, "Private Information") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

2. Defendant is the ninth largest global property and casualty insurer with more than 40,000 employees that generates more than $50 billion in annual consolidated revenue.[1]

3. On or around April 30, 2026, the notorious criminal ransomware group known as "Everest" accessed Defendant's or its third-party vendor's computer network and then targeted

[1] *Liberty Mutual Insurance*, LINKEDIN, https://www.linkedin.com/company/liberty-mutual-insurance/ (last visited May 5, 2025).

and exfiltrated the Private Information of Liberty Mutual's current and former clients (the "Data Breach").[2]

4. Plaintiffs have since discovered that Everest has added Defendant to its dark web leak site, where their Private Information, including their highly sensitive medical records, may be posted for any nefarious actor to view, download, and use to commit crimes against Plaintiffs and Class Members, including identity theft and fraud.[3]

5. Defendant has yet to provide direct notice to those impacted, leaving victims in the dark of their increased risk of imminent fraud and identity theft.

6. Defendant failed to adequately protect Plaintiffs' and Class Members' Private Information—and failed to even encrypt or redact this highly sensitive information. This unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect its clients' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

7. Plaintiffs bring this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; (iii) effectively implement security procedures free of

[2] Marianne Kolbasuk McGee, *Everest Group Begins Leaking Alleged Liberty Mutual Data*, BANK INFO SECURITY (May 4, 2026), https://www.bankinfosecurity.com/everest-group-begins-leaking-alleged-liberty-mutual-data-a-31589.

[3] Stefanie Schappert, *Liberty Mutual ransomware attack exposes thousands of policyholders, hackers claim*, CYBERNEWS (May 1, 2026), https://cybernews.com/security/liberty-mutual-ransomware-attack-policyholder-data/.

vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

8. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) 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 backed up 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.

9. Plaintiffs are clients of Defendant and a Data Breach victims. They bring this class action on behalf of themselves, and all others harmed by Defendant's misconduct.

10. The exposure of one's Private Information to cybercriminals is a bell that cannot be unrung. Before this data breach, Defendant's current and former clients' Private Information was exactly that—private. Not anymore. Now, their sensitive data is forever exposed and unsecure.

PARTIES

11. Plaintiff, Robert Francis, is a natural person and citizen of Massachusetts, where he intends to remain.

12. Plaintiff, John Goodwin, is a natural person and citizen of Massachusetts, where he intends to remain.

13. Defendant Liberty Mutual Insurance Company is a corporation incorporated under the laws of the Commonwealth of Massachusetts with its principal place of business at 175

Berkeley Street, Boston, Massachusetts 02116.

JURISDICTION & VENUE

14. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Plaintiffs and at least one member of the putative class are citizens of different states and there are over 100 putative Class Members.

15. This Court has personal jurisdiction over Defendant because it is headquartered in Massachusetts and regularly conducts business in Massachusetts.

16. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

Liberty Mutual

17. Liberty Mutual is a Fortune 100 insurance company headquartered in Boston, Massachusetts. Defendant offers a wide range of insurance products and services, including personal, automobile, homeowners, specialty, reinsurance, commercial multiple-peril, workers' compensation, commercial automobile, general liability, surety and commercial.[4] Liberty Mutual states that "our customers and our reach span the globe"[5] and boasts that holds $124 billion in assets under management.[6]

---

[4] *2024 Purpose & Impact Report* at 6, LIBERTY MUTUAL, https://www.libertymutualgroup.com/documents/2024-purpose-and-impact-report.pdf (last visited May 5, 2026).

[5] *Business Summary*, LIBERTY MUTUAL, https://www.libertymutualgroup.com/about-lm/corporate-information/business-summary (last visited May 5, 2026).

[6] *Liberty Mutual Investments Annual Report 2025*, LIBERTY MUTUAL, https://www.libertymutualinvestments.com/2025-annual-report (last visited May 5, 2026).

18. On information and belief, Liberty Mutual accumulates highly sensitive Private Information of its current and former clients.

19. In collecting and maintaining its clients' Private Information, Defendant agreed it would safeguard the data in accordance with state law and federal law. After all, Plaintiffs and Class Members themselves took reasonable steps to secure their Private Information.

20. Liberty Mutual understood the need to protect its current and former clients' Private Information and prioritize its data security.

21. Indeed, Liberty Mutual states in its Privacy Policy for Mutual Personal Lines that:

a. "We value you as a customer and take your personal privacy seriously;" and

b. "We maintain physical, electronic, and procedural safeguards to protect your nonpublic personal information. These safeguards comply with applicable laws. Our employees and agents are authorized to access your data only for legitimate business purposes."[7]

22. Despite recognizing its duty to do so, on information and belief, Liberty Mutual has not implemented reasonably cybersecurity safeguards or policies to protect clients' Private Information, adequately supervised its third-party agents or adequately trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Liberty Mutual leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to clients' Private Information.

[7] *Liberty Mutual Personal Lines – Notice of Privacy Policy and Insurance Information Practices*, LIBERTY MUTUAL, https://www.libertymutualgroup.com/general/about-lm/corporate-information/liberty-mutual-personal-lines-notice-privacy-policy-and-insurance-information-practices (last visited May 5, 2026).

Liberty Mutual Fails to Safeguard Clients' Private Information

23. On or before April 30, 2026, the notorious criminal ransomware group known as Everette accessed Defendant's or its third-party vendor's computer network and stole the Private Information stored therein. The Data Breach resulted in the Private Information of current and former clients of Defendant being exposed to cybercriminals.

24. According to the Health Sector Cybersecurity Coordination Center ("HC3"), Everest exploits legitimate compromised user accounts to gain access to a company's network and then accesses multiple systems within the target organization.[8] To avoid detection, Everest routinely removes tools, reconnaissance output files, and data collection archives from compromised hosts to cover their tracks and maintain persistence within the network.[9] The group then installs a file archiver on servers to archive data for exfiltration.[10] The data is then transferred out of the network for ransom or sale.[11]

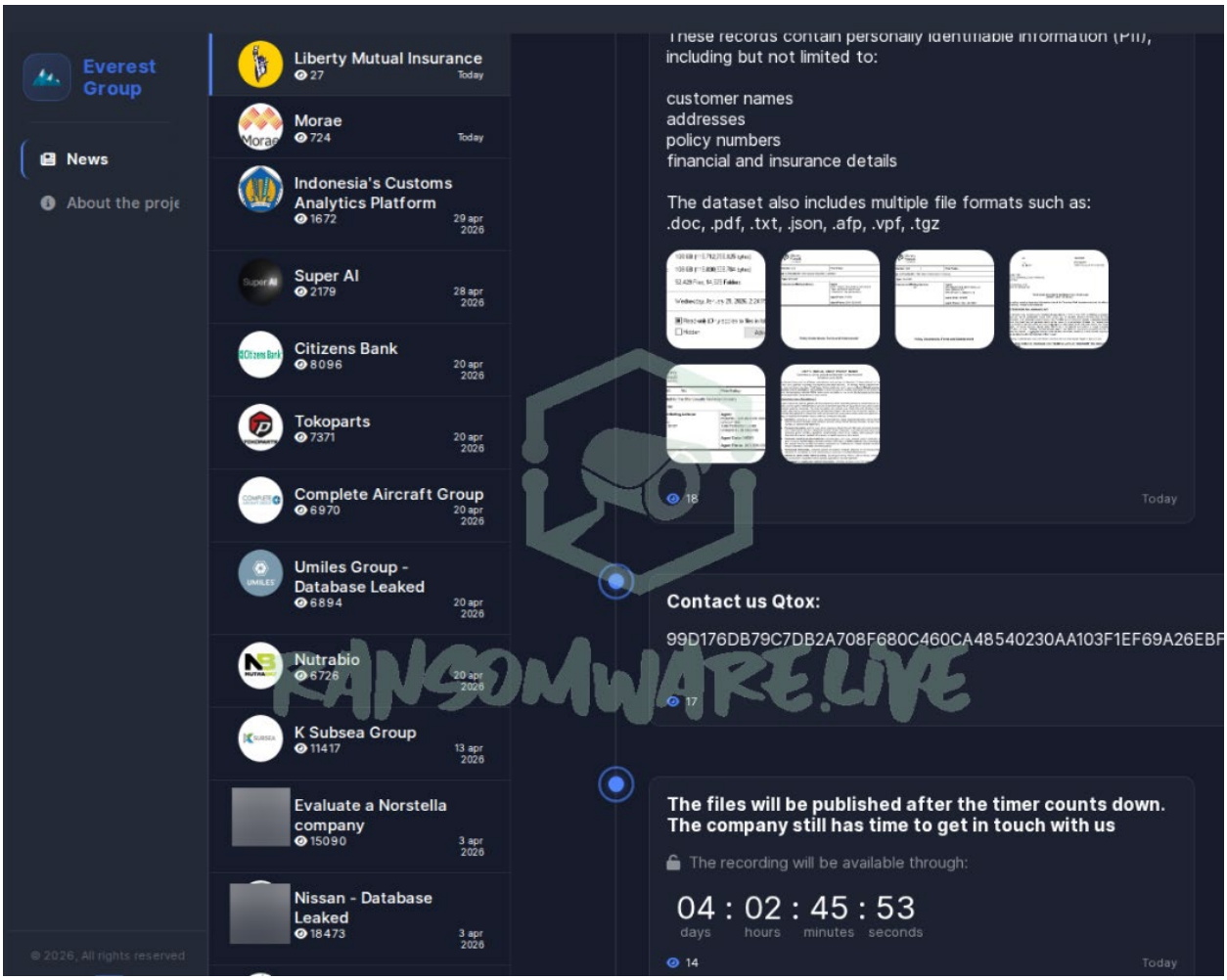
25. Once the files are stolen, Everest demands a ransom payment from the hacked organization, threatening to publish the stolen data if the ransom demand is not met.[12]

26. The group maintains a data leak site on the dark web to publish stolen information and advertise access to compromised networks.[13]

---

[8] *Threat Actor Profile: Everest Ransomware Group*, HC3 (Aug. 20, 2024), https://www.hipaajournal.com/wp-content/uploads/2024/08/hhs-hc3-everest-ransomware-group-threat-profile-aug-2024.pdf .
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Everest*, BLACKFOG, https://www.blackfog.com/cybersecurity-101/everest/ (last visited May 5, 2026).
[13] *Everest*, RANSOMLOOK, https://www.ransomlook.io/group/everest (last visited May 5, 2026).

27. On or around April 30, 2026, Everest posted on its dark web leak site that it had hacked Defendant.[14]



28. Everest's post displayed Defendant's name and logo, and stated "[t]hese records contain personally identifiable information (PII), including but not limited to: customer names, addresses, policy numbers, financial and insurance details."[15]

[14] *Liberty Mutual Insurance*, RANSOMWARE.LIVE, https://www.ransomware.live/id/TGliZXJ0eSBNdXR1YWwgSW5zdXJhbmNlQGV2ZXJlc3Q= (last visited May 5, 2026).
[15] *Id.*

29. The post additionally stated, "[t]he files will be published after the timer counts down. The company still has time to get in touch with us." The post also displayed a countdown clock displaying "04 days," "02 hours," 45 minutes," and "53 seconds."[16]

30. Since this deadline has since passed, on information and belief, Plaintiffs' and the Class's Private Information has already been published or otherwise disseminated on the dark web.

31. According to Cybernews, Everest's post further claims to have stolen a 108 GB cache of data from Defendant – the equivalent of 52,429 files, or 14,979 folders.[17] Everest also stated that the stolen dataset contains "tens of thousands" of insurance-related documents, including customer-facing records, individual policy documents, and generated forms.[18]

32. Thus, Everest employed tried and tested ransomware tactics in the Data Breach: it hacked Defendant's system to gain access to its network, it targeted and encrypted Plaintiffs' and the Class's Private Information once inside, and it subsequently exfiltrated the data.

33. As Everest's post makes clear, it is following is the *modus operandi* of ransomware groups to contact the hacked organization and demand a ransom payment, threatening to publish the stolen data if such a payment is not made.

34. On information and belief, Defendant has not made any public statements regarding whether it made a ransom payment.

35. However, even if Defendant makes a ransom payment, there is no guarantee that the Private Information stolen in the Data Breach will be deleted.[19] The stolen data is valuable, and

---

[16] *Id.*
[17] *See Liberty Mutual ransomware attack exposes thousands of policyholders, hackers claim*, n. 3 *supra*.
[18] *Id.*
[19] Steve Adler, *Majority of Ransomware Victims That Pay a Ransom Suffer a Second Attack*, THE HIPAA JOURNAL (Feb. 23, 2024), https://www.hipaajournal.com/majority-of-ransomware-victims-that-pay-a-ransom-suffer-a-second-attack/.

can easily be sold to another threat actor, so there is little incentive to delete it.[20]

36. Because of the Data Breach, Defendant's clients' names, dates of birth, Social Security numbers and other Private Information, such as their sensitive medical and financial records, were posted, or will be imminently posted, on the dark web, where they remain available for untold fraud and identity theft.

37. Worse still, Defendant has yet to provide direct written notice to Plaintiffs and Class Members that their Private Information was taken without authorization, leaving them unaware of the need to take prompt action to protect themselves from further harm.

38. Because of the Data Breach and Defendant's failure to provide proper and timely notice, Plaintiffs and Class Members are, and will remain, at risk that their data will be illegally used imminently and in the future.

39. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[21]

40. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiffs' and the Class's Private Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiffs' and the Class's financial accounts.

---

[20] *Id*.

[21] Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back.

41. On information and belief, Liberty Mutual failed to adequately train and/or supervise its IT and data security employees (or third-party agents) on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its clients' Private Information. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing its clients' Private Information.

Plaintiffs' Experiences and Injuries

Plaintiff Robert Francis

42. Plaintiff Robert Francis is a client of Defendant, holding three policies with Liberty Mutual through his employer.

43. Thus, Defendant obtained and maintained Plaintiff Francis's Private Information.

44. As a result, Plaintiff Francis was injured by Defendant's Data Breach.

45. As a condition of receiving insurance policies from Defendant, Plaintiff Francis provided Defendant (or its third-party agent) with his Private Information and allowed it to maintain his Private Information. Defendant (or its third-party agent) used Plaintiff Francis's Private Information to facilitate its provision of insurance services and to operate its business.

46. Plaintiff Francis provided Defendant with at least his name, date of birth, Social Security number, financial information, health insurance information, address, and contact information.

47. Plaintiff Francis trusted that Defendant (or its third-party agent) would use reasonable measures to protect his Private Information according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Francis's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

48. Plaintiff Francis reasonably understood that a portion of the funds he paid towards his insurance premiums would be used to pay for adequate cybersecurity and protection of Private Information.

49. Defendant has yet to contact Plaintiff Francis about the Data Breach.

50. To the best of his knowledge, Plaintiff Francis has not experienced another data breach, other than the Data Breach at issue here.

51. On information and belief, because of the Data Breach, Plaintiff Francis's Private Information has already been published or otherwise disseminated—or will be published or otherwise disseminated imminently—by Everest or by other cybercriminals on the dark web.

52. As a result of the Data Breach Plaintiff Francis has spent—and will continue to spend—significant time and effort monitoring his accounts, his credit files and his financial statements to protect himself from fraud and identity theft.

53. In the aftermath of the Data Breach, Plaintiff Francis began experiencing spam, scam, and phishing text messages and phone calls. Plaintiff Francis reasonably believes that the spam, scam and phishing communications are the result of the Data Breach as they began in the days following the Data Breach and are being transmitted to the same contact number Plaintiff Francis provided to Defendant.

54. The unwanted communications Plaintiff Francis is receiving are a distraction, must be blocked, and waste Plaintiff Francis's time each day. Further, these spam, scam, and phishing calls and texts are evidence that Plaintiff Francis's Private Information is being exploited by cybercriminals.

55. Plaintiff Francis fears for the security of his Private Information and worries about what information was exposed in the Data Breach. Plaintiff Francis is especially concerned that

his sensitive health records will be made available on the dark web.

56. Because of Defendant's Data Breach, Plaintiff Francis has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Francis's injuries are precisely the type of injuries that the law contemplates and addresses.

57. Plaintiff Francis suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy.

58. Plaintiff Francis suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and medical identity theft—all because Defendant's Data Breach placed Plaintiff Francis's Private Information right in the hands of criminals.

59. Because of the Data Breach, Plaintiff Francis anticipates spending considerable amounts of time and money to try and mitigate his injuries.

60. Today, Plaintiff Francis has a continuing interest in ensuring that his Private Information—which, upon information and belief, remains backed up in Defendant' possession—is protected and safeguarded from additional breaches.

Plaintiff John Goodwin

61. Plaintiff John Goodwin is a former client of Defendant, having held multiple auto policies with Liberty Mutual from on or around 2016 to on or around 2023.

62. Thus, Defendant obtained and maintained Plaintiff Goodwin's Private Information.

63. As a result, Plaintiff Goodwin was injured by Defendant's Data Breach.

64. As a condition of receiving insurance policies from Defendant, Plaintiff Goodwin provided Defendant (or its third-party agent) with his Private Information and allowed it to maintain his Private Information. Defendant (or its third-party agent) used Plaintiff Goodwin's Private Information to facilitate its provision of insurance services and to operate its business.

65. Plaintiff Goodwin provided Defendant with at least his name, date of birth, Social Security number, driver's license number, financial information, address, and contact information.

66. Plaintiff Goodwin trusted that Defendant (or its third-party agent) would use reasonable measures to protect his Private Information according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Goodwin's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

67. Plaintiff Goodwin reasonably understood that a portion of the funds he paid towards his insurance premiums would be used to pay for adequate cybersecurity and protection of Private Information.

68. Defendant has yet to contact Plaintiff Goodwin about the Data Breach.

69. On information and belief, because of the Data Breach, Plaintiff Goodwin's Private Information has already been published or otherwise disseminated—or will be published or otherwise disseminated imminently—by Everest or by other cybercriminals on the dark web.

70. On or around April 2026, Plaintiff Goodwin experienced fraudulent charges made to his checking account. As a result of the fraudulent charges, Plaintiff Goodwin was forced to spend time on the phone with his financial institution reporting the fraud, cancelling the affected debit card, and replacing the card.

71. As a result of the fraud he experienced, Plaintiff Goodwin has spent—and will continue to spend—significant time and effort monitoring his accounts, his credit files and his financial statements to protect himself from fraud and identity theft.

72. In the aftermath of the Data Breach, Plaintiff Goodwin began experiencing a major increase in scam and spam and phone calls. Plaintiff Goodwin reasonably believes that the spam,

and scam calls are the result of the Data Breach as they began in the days following the Data Breach and are being transmitted to the same contact number Plaintiff Goodwin provided to Defendant.

73. The unwanted communications Plaintiff Goodwin is receiving are a distraction, must be blocked, and waste Plaintiff Goodwin's time each day. Further, these spam and scam calls are evidence that Plaintiff Goodwin's Private Information is being exploited by cybercriminals.

74. Plaintiff Goodwin fears for the security of his Private Information and worries about what information was exposed in the Data Breach.

75. Because of Defendant's Data Breach, Plaintiff Goodwin has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Goodwin's injuries are precisely the type of injuries that the law contemplates and addresses.

76. Plaintiff Goodwin suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy.

77. Plaintiff Goodwin suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and medical identity theft—all because Defendant's Data Breach placed Plaintiff Goodwin's Private Information right in the hands of criminals.

78. Because of the Data Breach, Plaintiff Goodwin anticipates spending considerable amounts of time and money to try and mitigate his injuries.

79. Today, Plaintiff Goodwin has a continuing interest in ensuring that his Private Information—which, upon information and belief, remains backed up in Defendant' possession—is protected and safeguarded from additional breaches.

Defendant Knew, Or Should Have Known, of the Risk Because Insurance Entities in Possession of Private Information Are Particularly Susceptible to Cyber Attacks

80. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they custody. 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.

81. In 2024, a 3,158 data breaches occurred, exposing approximately 1,350,835,988 sensitive records—a 211% increase year-over-year.

82. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting the insurance industry and insurance companies that collect and store Private Information, like Defendant, preceding the date of the breach.

83. According to the Casualty Actuarial Society, the industry remains a prime target for cyberattacks as insurance companies hold vast and rich databases that are goldmines of personal information for malicious actors.[22] They are also highly liquid entities with large cash reserves.[23]

84. Indeed, in June 2025, Aflac, Philadelphia Insurance, and Erie Insurance were all struck by attacks that disrupted their networks and systems.[24] The following month, Allianz Life suffered an attack involving a third-party vendor where hackers used social engineering to access a cloud-based customer relationship management (CRM) system, putting millions of sensitive

[22] Feras Samain, *Caught in the Web: Targeted Cyber Attacks on Insurers*, CASUALTY ACTUARIAL SOCIETY (Oct. 17, 2025), https://ar.casact.org/caught-in-the-web-targeted-cyber-attacks-on-insurers/.
[23] *Id.*
[24] *Id.*

personal records at risk.[25]

85. Actuaries are uniquely positioned to not only help reduce the risk of cyberattacks, but to assess and quantify cyber risk.[26] They have access to, and handle, sensitive data that feeds their analyses and models and can take precautionary steps such as anonymizing personally identifiable information, or using synthetic data, can help reduce the risk of exposure.[27]

86. In 2025, to warn insurance companies against the dangers of cyberattacks and to provide best practices on cybersecurity, the Casualty Actuarial Society released a report, that, among other things, detailed how prevention of cyberattacks can be used as a risk mitigation or risk management strategy.[28]

87. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) ransomware actors were targeting entities such as Defendant, (ii) ransomware gangs were ferociously aggressive in their pursuit of entities such as Defendant, (iii) ransomware gangs were leaking corporate information on dark web portals, and (iv) ransomware tactics included threatening to release stolen data.

88. In light of the information readily available and accessible on the internet before the Data Breach, Defendant, having elected to store the unencrypted Private Information of thousands of its current and former clients in an Internet-accessible environment, had reason to be on guard for the exfiltration of the Private Information and Defendant's type of business had cause to be particularly on guard against such an attack.

---

[25] *Id.*
[26] *Id.*
[27] *Id.*
[28] Olivier Lopez et al., *Cyber Risk: Quantification, Stress Scenarios, Mitigation, And Insurance*, CASUALTY ACTUARIAL SOCIETY (2025), https://www.casact.org/sites/default/files/2025-06/CAS_Research_Paper-on_Cyber-Risk-Final.pdf.

89. Before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' Private Information could be accessed, exfiltrated, and published as the result of a cyberattack. Notably, data breaches are prevalent in today's society therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

90. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted its clients' Social Security numbers and other sensitive data elements within the Private Information to protect against their publication and misuse in the event of a cyberattack.

Consumers Prioritize Data Security

91. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year "Consumer Privacy Survey."[29] Therein, Cisco reported the following:

a. For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data."[30]

b. "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly."[31]

c. 89% of consumers stated that "I care about data privacy."[32]

d. 83% of consumers declared that "I am willing to spend time and money to protect

[29] *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited March 19, 2025).
[30] *Id*. at 3.
[31] *Id*.
[32] *Id*. at 9.

data" and that "I expect to pay more" for privacy.33

e. 51% of consumers revealed that "I have switched companies or providers over their data policies or data-sharing practices."34

f. 75% of consumers stated that "I will not purchase from organizations I don't trust with my data."35

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

92. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their Private Information that can be directly traced to Defendant.

93. As a result of Liberty Mutual's failure to prevent the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiffs and the class have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their Private Information is used;

b. The diminution in value of their Private Information;

c. The compromise and continuing publication of their Private Information;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

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

[33] *Id*.
[34] *Id*.
[35] *Id*. at 11.

fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen Private Information; and

h. The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Private Information in its possession.

94. Stolen Private Information is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen Private Information can be worth up to $1,000.00 depending on the type of information obtained.

95. The value of Plaintiffs' and the proposed Class's Private Information on the black market is considerable. Stolen Private Information trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

96. Social Security numbers are particularly attractive targets for hackers because they can easily be used to perpetrate identity theft and other highly profitable types of fraud. Moreover, Social Security numbers are difficult to replace, as victims are unable to obtain a new number until the damage is done.

97. It can take victims years to spot identity or Private Information theft, giving criminals plenty of time to use that information for cash.

98. One such example of criminals using Private Information for profit is the development of "Fullz" packages.

99. Cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

100. The development of "Fullz" packages means that stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and the Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs' and members of the Class's stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

101. Defendant disclosed the Private Information of Plaintiffs and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the Private Information of Plaintiffs and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Private Information.

102. Defendant's failure to properly notify Plaintiffs and the Class of the Data Breach exacerbated Plaintiffs' and the Class's injuries by depriving them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate

the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

103. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of Private Information.

104. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

105. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

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

107. 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.

108. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to clients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

109. Several best practices have been identified that—at a minimum—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

110. Other industry standard best practices include: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

111. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

112. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

113. Plaintiffs bring this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), individually and on behalf of all members of the following "Classes":

> **Nationwide Class:** All individuals residing in the United States whose Private Information was compromised in the Data Breach, including all those individuals who received a Notice.
>
> **Massachusetts Subclass**: All individuals residing in Massachusetts whose Private Information was compromised in the Data Breach, including all those individuals who received a Notice.

114. 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 a 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; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

115. Plaintiffs reserve the right to modify or amend the definition of the proposed Classes before the Court determines whether certification is appropriate should discovery reveal that the Classes should include further categories of individuals.

116. The proposed Classes meet the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

117. Ascertainability. This action is brought and may be maintained as a class action because there is a well-defined community of interest among many persons who comprise a readily ascertainable class. A well-defined community of interest exists to warrant class-wide relief because Plaintiffs and all Class Members were subjected to the same wrongful practices by Defendant, entitling them to the same relief. All members of the proposed Classes are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them Data Breach Notices.

118. Numerosity. The Class is so numerous that individual joinder of its members is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, Defendant reported that the Private Information of at least 15,630 individuals throughout the United States was compromised in the Data Breach.

119. Typicality. Plaintiffs' claims are typical of Class Members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

120. Adequacy. Plaintiffs will fairly and adequately protect the proposed Classes' common interests. Their interests do not conflict with Class Members' interests. And Plaintiffs has retained counsel—including Interim Lead Counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Classes' behalf.

121. Commonality and Predominance. Plaintiffs' and the Classes' claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class Members—for which a class wide proceeding can answer for all Plaintiffs and Class Members. In fact, a class wide proceeding is necessary to answer the following questions:

a. Whether and to what extent Defendant had a duty to protect the Private

Information of Plaintiffs and Class Members;

b. Whether Defendant had a duty not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the Private Information of Plaintiffs and Class Members for non-business purposes;

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

e. When Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;

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

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

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual damages, nominal damages, and/or statutory damages as a result of Defendant 'wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution because of Defendant' wrongful conduct; and

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced because of the Data Breach.

122. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class Members, on an individual basis, to obtain effective redress for their injuries. Not only would individual litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiffs and the Classes)

123. Plaintiffs incorporate by reference paragraphs 1-122 as if fully set forth herein.

124. This is a claim for negligence is made on behalf of Plaintiffs and the Classes.

125. Plaintiffs and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would safeguard their Private Information, use their Private Information for business purposes only, and/or not disclose their Private Information to unauthorized third parties.

126. Defendant owed a duty of care to Plaintiffs and Class Members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their Private Information in a data breach.

127. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if their Private Information was wrongfully disclosed.

128. Defendant owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices.

129. After all, Defendant actively sought and obtained Plaintiffs' and Class Members' Private Information.

130. Defendant owed—to Plaintiffs and Class Members—at least the following duties to:

a. exercise reasonable care in handling and using the Private Information in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably

c. protect the information from a data breach, theft, and unauthorized;

d. promptly detect attempts at unauthorized access; and notify Plaintiffs and Class members within a reasonable timeframe of any breach to the security of their Private Information.

131. Also, Defendant owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs and Class Members to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

132. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain under applicable regulations.

133. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

134. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Private Information, a necessary part of doing business with Defendant.

135. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that Defendant holds vast amounts of Private Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Private Information —whether by malware or otherwise.

136. Private Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiffs' and Class Members' and the importance of exercising reasonable care in handling it.

137. Defendant improperly and inadequately safeguarded the Private Information of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

138. Defendant breached these duties as evidenced by the Data Breach.

139. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class Members' Private Information by:

140. disclosing and providing access to this information to third parties and

141. failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

142. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the Private Information of Plaintiffs and Class Members which actually and proximately caused the Data Breach and Plaintiffs' and Class Members' injury.

143. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and Class Members' injuries-in-fact.

144. Defendant has admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

145. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class Members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

146. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and Class Members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Private Information by criminals, improper disclosure of their Private Information, lost benefit of their bargain, lost value of their Private Information, the use of their Private Information to attempt fraudulent transactions (Plaintiffs Morton) and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's

negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CLAIM FOR RELIEF
Negligence *Per Se*
(On Behalf of Plaintiffs and the Classes)

147. Plaintiffs incorporate by reference paragraphs 1-122 as if fully set forth herein.

148. This is a claim for negligence *per se* is made on behalf of Plaintiffs and the Classes.

149. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

150. Section 5 of the FTC Act 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 the Private Information entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs' and the Class Members' sensitive Private Information.

151. Defendant breached its respective duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Private Information.

152. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information Defendant had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

153. The harm that has occurred is the type of harm the FTC Act is intended to guard

against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and members of the Class.

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

155. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their Private Information.

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

157. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will continue to suffer numerous injuries (as detailed supra).

THIRD CLAIM FOR RELIEF
Breach of Implied Contract
(On Behalf of Plaintiffs and the Classes)

158. Plaintiffs incorporate by reference paragraphs 1-122 as if fully set forth herein.

159. This is a claim for breach of implied contract is made on behalf of Plaintiffs and the Classes.

160. Defendant (or its third-party agents) required Plaintiffs and members of the Class (or their third-party agents) to provide Defendant with their Private Information as a condition of participating in the insurance plans administered by Defendant.

161. In turn, Defendant agreed it would not disclose the Private Information it collects to unauthorized persons. Defendant also promised to safeguard claimants' Private Information.

162. Plaintiffs and the members of the Class (or their third-party agents) accepted Defendant's (or its third-party agent's) offer by providing Private Information to Defendant in exchange for participating in the insurance plans administered by Defendant.

163. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their Private Information.

164. Plaintiffs and the members of the Class (or their third-party agents) would not have entrusted their Private Information to Defendant (or its third-party agents) in the absence of such an agreement with Defendant.

165. Defendant materially breached the contracts it had entered with Plaintiffs and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant also breached the implied contracts with Plaintiffs and members of the Class by:

166. Failing to properly safeguard and protect Plaintiffs' and members of the Class's Private Information;

167. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

168. Failing to ensure the confidentiality and integrity of electronic Private Information that Defendant created, received, maintained, and transmitted.

169. The damages sustained by Plaintiffs and members of the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

170. Plaintiffs and members of the Class have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

171. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon 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 in addition to its form.

172. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

173. Defendant failed to advise Plaintiffs and members of the Class of the Data Breach promptly and sufficiently.

174. In these and other ways, Defendant violated its duty of good faith and fair dealing.

175. Plaintiffs and members of the Class have sustained damages because of Defendant's breaches of its agreement, including breaches of it through violations of the covenant of good faith and fair dealing.

176. Plaintiffs, on behalf of themselves and the Class, seek compensatory damages for breach of implied contract, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

FOURTH CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of Plaintiffs and the Classes)

177. Plaintiffs incorporate by reference paragraphs 1-122 as if fully set forth herein.

178. This is a claim for unjust enrichment is made on behalf of Plaintiffs and the Classes.

179. This claim is plead in the alternative to the breach of implied contractual duty claim.

180. Plaintiffs and members of the Class conferred a benefit upon Defendant in the form of participating in the insurance plans it administers. Defendant therefore benefited from the receipt of Plaintiffs' and the Class's Private Information. Defendant appreciated or had knowledge of the benefits conferred upon itself by Plaintiffs and members of the Class.

181. Under principals of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and the proposed Class's Private Information because Defendant failed to adequately protect their Private Information. Plaintiffs and the proposed Class (or their third-party agents) would not have provided their Private Information had they known Defendant would not adequately protect their Private Information.

182. Defendant should be compelled to disgorge into a common fund to benefit Plaintiffs and members of the Class all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged here.

FIFTH CLAIM FOR RELIEF
Invasion of Privacy
(On Behalf of Plaintiffs and the Class)

183. Plaintiffs incorporate by reference paragraphs 1-122 as if fully set forth herein.

184. This is a claim for invasion of privacy is made on behalf of Plaintiffs and the Classes.

185. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential Private Information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

186. Defendant owed a duty to the claimants participating in the insurance plans it administers, including Plaintiffs and the Class, to keep this information confidential.

187. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs' and Class Members' Private Information is highly offensive to a reasonable person.

188. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class (or their third-party agents) disclosed their sensitive and confidential information to Defendant as part of participating in the insurance plans Defendant administers, but they did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

189. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

190. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

191. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

192. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

193. As a proximate result of Defendant's acts and omissions, the Private Information of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

194. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class because their Private Information is still maintained by Defendant with its inadequate cybersecurity system and policies.

195. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the Private Information of Plaintiffs and the Class.

196. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other members of the Class, also seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

SEVENTH CAUSE OF ACTION
Violation of the Massachusetts Consumer Protection Act
Ch. 93A § 1, et seq.
(On Behalf of Plaintiffs and the Nationwide Class or, in the alternative, on behalf of Plaintiffs and the Massachusetts Subclass)

197. Plaintiffs incorporate paragraphs 1-122 above as though fully set forth herein.

198. This is a claim for Plaintiffs and the Nationwide Class or, in the alternative, for Plaintiffs and the Massachusetts Subclass.

199. Defendant, Plaintiffs, and Class Members (or Massachusetts Subclass Members) are each a "person" as defined by the Massachusetts Consumer Protection Act ("MCPA"), MASS. GEN. LAWS Ch. 93A, §1(a).

200. By advertising and selling insurance policies throughout the state, Defendant is engaged in "trade" or "commerce" defined as "the advertising, the offering for sale, rent or lease, the sale, rent, lease or distribution of any services and any property, tangible or intangible, real, personal or mixed, any security . . . and any contract of sale of a commodity for future delivery, and any other article, commodity, or thing of value wherever situate, and shall include any trade or commerce directly or indirectly affecting the people of this commonwealth." MASS. GEN. LAWS Ch. 93A, §1(b).

201. Defendant (or its third-party agent) obtained Plaintiffs' and Class Members' (or Massachusetts Subclass Members') Private Information as a result of selling and administering insurance policies, and for other business-related reasons, all of whom are Plaintiffs and Class Members (or Massachusetts Subclass Members), and the Data Breach occurred at least in part through the use of the internet, an instrumentality of interstate commerce.

202. Defendant is engaged in trade or commerce that directly or indirectly affects people of the Commonwealth of Massachusetts. Defendant is headquartered in Massachusetts, but has other offices in the United States.

203. Under MASS. GEN. LAWS Ch. 93A, §2(a), "unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."

204. Defendant violated MASS. GEN. LAWS Ch. 93A, §2(a) in that it has engaged in "unfair or deceptive acts or practices in the conduct of any trade or commerce."

205. Defendant had a duty to keep the Private Information of Plaintiffs and Class Members (or Massachusetts Subclass Members) safe and secure under the various laws and regulations discussed hereinabove.

206. Defendant failed to adequately protect and secure the Private Information of Plaintiffs and Class Members (or Massachusetts Subclass Members) and failed to comply with its obligations to protect and secure the Private Information.

207. Defendant failed to comply with industry standards for the protection and security of the Private Information.

208. Defendant failed to comply with its own privacy practices relating to the protection and security of the Private Information.

209. Defendant failed to disclose that it (or its third-party agent) did not have adequate security practices in place to safeguard the Private Information.

210. Criminals were able to access the Private Information through the Data Breach.

211. Defendant had a duty to timely notify its clients, including Plaintiffs and Class Members (or Massachusetts Subclass Members), of the Data Breach, including under MASS. GEN. LAWS Ch. 93H, §3, the Massachusetts Security Breach statute.

212. Defendant failed to timely notify its clients, including Plaintiffs and Class Members (or Massachusetts Subclass Members), of the Data Breach.

213. The aforementioned actions and omissions constitute unfair or deceptive acts or practices under MASS. GEN. LAWS Ch. 93A, §2(a).

214. Such acts by Defendant were likely to mislead a reasonable person who did business with Defendant.

215. Said acts are material in that a reasonable person would consider them important in deciding whether to purchase a insurance policy from Defendant (or its third-party agent) or to otherwise do business with Defendant. If Plaintiffs and Class Members (or Massachusetts Subclass Members) had known that Defendant (or its third-party agent) had inadequate computer systems and data security practices to properly safeguard their Private Information, they would not have purchased insurance products from Defendant or otherwise done business with Defendant.

216. Defendant acted with disregard for the security of Plaintiffs' and Class Members' (or Massachusetts Subclass Members') Private Information. Defendant knew or should have known that it (or its third-party agent) had inadequate computer systems and data security practices to safeguard such information, and Defendant knew or should have known that hackers were attempting to access the Private Information in large companies' databases, such as Liberty

Mutual's.

217. As a result of the actions and omissions alleged above, Plaintiffs and Class Members (or Massachusetts Subclass Members) have suffered, and will continue to suffer, injury in an amount to be determined at trial, including, but not limited to: the loss of the benefit of their bargain with Defendant; losses from fraud and identity theft; costs for credit monitoring and identity protection services; time and expenses incurred protecting themselves from fraudulent activity; loss of value of their Private Information; and an increased, imminent risk of fraud and identity theft.

218. As a result of the aforementioned actions and omissions, Plaintiffs and Class Members (or Massachusetts Subclass Members) seek their actual damages, statutory damages, double or treble damages, their costs and reasonable attorneys' fees, and any injunctive or equitable relief needed to secure Private Information in the possession, custody, and control of Defendant and its agents. *See* MASS. GEN. LAWS Ch. 93A, § 9.

219. Further, as a direct result of Defendant's violations of the MCPA, Plaintiffs and Class Members (or Massachusetts Subclass Members) are entitled to injunctive relief, including, but not limited to:

a. Ordering that Defendant implement measures that ensure that the Private Information of Defendant's current and former employees and their dependents, and others' who provided their Private Information for a business-related reason, is appropriately encrypted and safeguarded when stored on Defendant's network or systems;

b. Ordering that Defendant purge, delete, and destroy in a reasonable secure manner Private Information not necessary to be maintained;

c. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

d. Ordering Defendant to meaningfully educate its current and former customers about the threats they face as a result of the accessibility of their Private Information to third parties, as well as the steps Defendant's current and former customers must take to protect themselves.

220. A demand identifying the claimant and reasonably describing the unfair or deceptive act or practice and the injury suffered was mailed or delivered to Defendant prior to the filing of a pleading alleging this claim for relief. *See* MASS. GEN. LAWS Ch. 93A, § 9(3). By letter dated August 19, 2025, Plaintiffs, on behalf of themselves and Class Members (or Massachusetts Subclass Members), sent Defendant notice under this provision.

EIGHTH CAUSE OF ACTION
Declaratory Judgment Act
28 U.S.C. §§ 2201, et seq.
(On Behalf of Plaintiffs and the Classes)

221. Plaintiffs hereby repeat and reallege paragraphs 1-122 of this Complaint and incorporates them by reference herein.

222. This is a claim declaratory relief for Plaintiffs and the Classes.

223. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

224. Defendant owed a duty of care to Plaintiffs and Class Members, which required Defendant to adequately monitor and safeguard Plaintiffs' and Class Members' Private

Information.

225. Defendant still possesses the Private Information belonging to Plaintiffs and Class Members.

226. Plaintiffs allege that Defendant's data security measures remain inadequate. Furthermore, Plaintiffs and Class Members continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

227. As a result of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security.

228. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure Plaintiffs' and Class Members' Private Information under the common law, the FTC Act, and other state and federal laws and regulations, as set forth herein;

b. Defendant's existing data monitoring measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect individuals' Private Information; and

c. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiffs' and Class Members' Private Information.

229. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security protocols consistent with legal and industry standards to protect the data entrusted to it.

230. If an injunction is not issued, Plaintiffs and the Classes will suffer irreparable injury and lack an adequate legal remedy to prevent another data breach of Defendant's computer systems. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiffs and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

231. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiffs and Class Members' injuries.

232. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. The cost of Defendant's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendant have a pre-existing legal duty to employ such measures.

233. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach of Defendant's systems and network, thus preventing future injury to Plaintiffs and other Class Members whose Private Information would be further compromised.

234. Following the issuance of the declaratory relief requested herein, pursuant to 28 U.S.C. § 2202, Plaintiffs and Class Members will seek any further necessary or proper relief, including damages, after reasonable notice and hearing, against Defendant.

PRAYER FOR RELIEF

Plaintiffs and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class,

appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Breach and the stolen Private Information;

E. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiffs hereby demand that this matter be tried before a jury.

Dated: May 5, 2026,

Respectfully submitted,

/s/ Casondra Turner
Casondra Turner (MA BBO No. 687682)
MILBERG, PLLC
260 Peachtree Street NW, Suite 2200
Atlanta, GA 30303
Telephone: (771) 772-3086
Email: cturner@milberg.com

Raina Borrelli (*Pro Hac Vice* forthcoming)
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
(872) 263-1100
(872) 263-1109 (facsimile)
raina@straussborrelli.com

* *Pro hac vice forthcoming*

Attorneys for Plaintiffs and Proposed Class

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

ROBERT FRANCIS and JOHN GOODWIN, on behalf of themselves and all others similarly situated,

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Casondra Turner; MILBERG, PLLC
260 Peachtree Street NW, Suite 2200; Atlanta, GA 30303;
Telephone: (771) 772-3086; Email: cturner@milberg.com

DEFENDANTS

LIBERTY MUTUAL INSURANCE COMPANY

County of Residence of First Listed Defendant Suffolk County, MA
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

Unknown

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)

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 $ 5000000

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

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
May 6, 2026

SIGNATURE OF ATTORNEY OF RECORD
/s/ Casondra Turner

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.

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

1. **Title of case (name of first party on each side only)** Robert Francis & John Goodwin vs. Liberty Mutual Insurance Company

2. **Category in which the case belongs based upon the numbered nature of suit code listed on the civil cover sheet. (See local rule 40.1(a)(1)).**

☐ **I.** **160, 400, 410, 441, 535, 830*, 835*, 850, 880, 891, 893, R.23, REGARDLESS OF NATURE OF SUIT.**

☐ **II.** **110, 130, 190, 196, 370, 375, 376, 440, 442, 443, 445, 446, 448, 470, 751, 820*, 840*, 895, 896, 899.**

☑ **III.** **120, 140, 150, 151, 152, 153, 195, 210, 220, 230, 240, 245, 290, 310, 315, 320, 330, 340, 345, 350, 355, 360, 362, 365, 367, 368, 371, 380, 385, 422, 423, 430, 450, 460, 462, 463, 465, 480, 485, 490, 510, 530, 540, 550, 555, 560, 625, 690, 710, 720, 740, 790, 791, 861-865, 870, 871, 890, 950.**
***Also complete AO 120 or AO 121. for patent, trademark or copyright cases.**

3. **Title and number, if any, of related cases. (See local rule 40.1(g)). If more than one prior related case has been filed in this district please indicate the title and number of the first filed case in this court.**

4. **Has a prior action between the same parties and based on the same claim ever been filed in this court?**
YES ☐ **NO** ☑

5. **Does the complaint in this case question the constitutionality of an act of congress affecting the public interest? (See 28 USC §2403)**
YES ☐ **NO** ☑
If so, is the U.S.A. or an officer, agent or employee of the U.S. a party?
YES ☐ **NO** ☐

6. **Is this case required to be heard and determined by a district court of three judges pursuant to title 28 USC §2284?**
YES ☐ **NO** ☑

7. **Do all of the parties in this action, excluding governmental agencies of the United States and the Commonwealth of Massachusetts ("governmental agencies"), residing in Massachusetts reside in the same division? - (See Local Rule 40.1(d)).**
YES ☐ **NO** ☑

A. **If yes, in which division do all of the non-governmental parties reside?**
Eastern Division ☐ **Central Division** ☐ **Western Division** ☐

B. **If no, in which division do the majority of the plaintiffs or the only parties, excluding governmental agencies, residing in Massachusetts reside?**
Eastern Division ☑ **Central Division** ☐ **Western Division** ☐

8. **If filing a Notice of Removal - are there any motions pending in the state court requiring the attention of this Court? (If yes, submit a separate sheet identifying the motions)**
YES ☐ **NO** ☐

(PLEASE TYPE OR PRINT)
ATTORNEY'S NAME Casondra Turner
ADDRESS 260 Peachtree Street NW, Suite 2200, Atlanta GA 30303
TELEPHONE NO. (771) 772-3086