CAUSE NO. _____

RAYMOND NEWSON, BRITTON BRYANT, DONALD TANNER, EDNA WHITTEN, FOLAYAN OAYNE, DRENETHA GOFF, KARA MONTAGUE, KARINA BARRATT, LYNDA ROBERTS, RANDY JACKSON, ROZALYNN FISHER, SHALENE WILLIS, and SHERIKA DODSON on behalf of themselves and all others similarly situated, Plaintiffs, v. **LANDMARK ADMIN, LLC, AMERICAN BENEFIT LIFE INSURANCE COMPANY, AMERICAN MONUMENTAL LIFE INSURANCE COMPANY, CAPITOL LIFE INSURANCE COMPANY, CONTINENTAL MUTUAL INSURANCE COMPANY, LIBERTY BANKERS LIFE INSURANCE COMPANY, and ACCENDO INSURANCE COMPANY,** Defendants.	IN THE DISTRICT COURT DALLAS COUNTY, TEXAS _____ JUDICIAL DISTRICT

CLASS ACTION PETITION

Plaintiffs Raymond Newson, Britton Bryant, Donald Tanner, Edna Whitten, Folayan Payne, Drenetha Goff, Kara Montague, Karina Barratt, Linda Roberts, Randy Jackson, Rozalynn Fisher, Shalene Willis, and Sherika Dodson ("Plaintiffs") bring this Class Action Petition against Landmark Admin, LLC ("Landmark"), Liberty Bankers Life Insurance Company, American Benefit Life Insurance Company, American Monumental Life Insurance Company, Capitol Life

Insurance Company, and Continental Mutual Insurance Company (collectively, "Liberty Bankers"), and Accendo Insurance Company ("Accendo") (together with Landmark and Liberty Bankers, the "Defendants") as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

DISCOVERY CONTROL PLAN

Due to the complexity of this case, discovery should be conducted pursuant to a discover control plan under Level 3, pursuant to Texas Rule of Civil Procedure 190.4. Plaintiffs affirmatively plead that this suit is not governed by the expedited actions process of Texas Rules of Civil Procedure 169 because Plaintiffs seek monetary relief in excess of $250,000.00.

SUMMARY OF ACTION

1. Plaintiffs bring this class action against Defendants for their failure to properly secure and safeguard sensitive information belonging to Plaintiffs and Class Members.

2. Landmark is a third-party administrator for insurance carriers.

3. Liberty Bankers is an insurance group that includes numerous insurance companies, including Liberty Bankers Life Insurance Company, American Monumental Life Insurance Company, Pellerin Life Insurance Company, American Benefit Life Insurance Company, Continental Mutual Insurance Company, and Capitol Life Insurance Company.

4. Accendo is a CVS Health Medicare supplement insurance provider.

5. Plaintiffs' and Class Members' (defined below) sensitive personal information—which they entrusted to Defendants on the mutual understanding that Defendants would protect it against disclosure—was targeted, unlawfully accessed, and exfiltrated due to the Data Breach.

6. The information compromised in the Data Breach included Plaintiffs' and Class Members' full names, driver's license numbers, passport numbers, tax identification numbers ("personally identifiable information" or "PII") and medical information, which is protected health information ("PHI" and, collectively with PII, the "Private Information") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

7. The Private Information compromised in the Data Breach was exfiltrated by, and remains in the hands of, cybercriminals who target Private Information for its value to identity thieves.

8. As a result of the Data Breach, Plaintiffs and approximately 1.6 million other Class Members[1] suffered concrete injuries, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) uncompensated 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) the dissemination of their Private Information on the dark web; (viii) experiencing an increase in spam calls, texts, and/or emails; (ix) nominal damages; and (x) 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 Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

[1]https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/2bd97a04-38be-40f1-94fd-9d143ea4bc9f.html

9. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect the Private Information entrusted to them from a foreseeable and preventable cyber-attack.

10. Moreover, upon information and belief, Defendants were targeted for a cyberattack due to its statuses as insurance companies and insurance administrators that collect and maintain highly valuable Private Information on its systems.

11. Defendants maintained, used, and shared the Private Information in a reckless manner. In particular, the Private Information was used and transmitted by Defendants in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendants, and thus, Defendants were on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

12. Defendants disregarded the rights of Plaintiffs and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

13. Plaintiffs' and Class Members' identities are now at risk because of Defendants' negligent conduct because the Private Information that Defendants collected and maintained has been accessed and acquired by data thieves.

14. Armed with the Private Information accessed in the Data Breach, data thieves have already engaged in identity theft and fraud and can in the future commit a variety of crimes

including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

15. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

16. Plaintiffs and Class Members may also incur out of pocket costs, *e.g.*, for purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

17. Plaintiffs bring this class action lawsuit on behalf all those similarly situated to address Defendants' inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

18. Through this Petition, Plaintiffs seek to remedy these harms on behalf of themselves and all other similarly situated individuals whose Private Information was accessed during the Data Breach.

19. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe and, as such, they also seek injunctive and other equitable relief.

JURISDICTION AND VENUE

20. This Court has subject matter jurisdiction over this controversy because the contracts between the parties were established in Texas. Moreover, the Defendants' collective alleged failure to adequately safeguard Class Members' data, *i.e.*, the site of Defendant Landmark's Data Breach, occurred in Texas and Plaintiffs have been damaged within the jurisdictional limits of this Court.

21. This Court has personal jurisdiction over Defendants because they are either a citizen of Texas or intentionally availed themselves to Texas through their course of business.

22. Venue is proper in this county under Tex. Civ. Prac. & Rem. Code § 15.002 because a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in Dallas County, Texas.

23. Pursuant to Texas Rule of Civil Procedure 47, Plaintiffs seek monetary relief over $1,000,000 for the class.

24. Upon information and belief, Plaintiffs' individual damages are less than $75,000.

PARTIES

25. Plaintiff Raymond Newson is, and at all relevant times has been, a resident and citizen of the State of California where he intends to remain.

26. Plaintiff Britton Bryant is, and at all relevant times has been, a resident and citizen of the State of South Carolina where he intends to remain.

27. Plaintiff Donald Tanner is, and at all relevant times has been, a resident and citizen of the State of Louisianna where he intends to remain.

28. Plaintiff Edna Whitten is, and at all relevant times has been, a resident and citizen of the State of Florida where she intends to remain.

29. Plaintiff Folayan Payne is, and at all relevant times has been, a resident and citizen of the State of Louisianna where he intends to remain.

30. Plaintiff Drenetha Goff is, and at all relevant times has been, a resident and citizen of the State of South Carolina where she intends to remain.

31. Plaintiff Kara Montague is, and at all relevant times has been, a resident and citizen of the State of Washington where she intends to remain.

32. Plaintiff Karina Barratt is, and at all relevant times has been, a resident and citizen of the State of South Carolina where she intends to remain.

33. Plaintiff Lynda Roberts is, and at all relevant times has been, a resident and citizen of the State of Louisianna where she intends to remain.

34. Plaintiff Randy Jackson is, and at all relevant times has been, a resident and citizen of the State of North Carolina where he intends to remain.

35. Plaintiff Rozalynn Fisher is, and at all relevant times has been, a resident and citizen of the State of California where she intends to remain.

36. Plaintiff Shalene Willis is, and at all relevant times has been, a resident and citizen of the State of New Jersey where she intends to remain.

37. Plaintiff Sherika Dodson is, and at all relevant times has been, a resident and citizen of the State of Pennsylvania where she intends to remain.

38. Liberty Bankers, an insurance group that includes numerous insurance company affiliates such as Liberty Bankers Life Insurance Company, American Monumental Life Insurance Company, Pellerin Life Insurance Company, American Benefit Life Insurance Company, Continental Mutual Insurance Company, and Capitol Life Insurance Company,[2] maintains its

[2] *See* https://lbig.com/about-us/company-affiliates (last accessed March 25, 2025).

principal place of business located at 1605 Lyndon B. Johnson Freeway, Suite 710, Dallas, Texas 75234. LBIG and its company affiliates can be served thru its registered agent National Registered Agents, Inc., 1999 Bryan Street, Suite 900, Dallas, Texas 75201.

39. Defendant Landmark is a limited liability company with its principal place of business located at 5750 County Rd 225, Brownwood, Texas 76801. The registered agent for service of process is Thomas A. Munson who can be served at the same address.

40. Defendant Accendo is an insurance company with its principal place of business located in West Valley City, Utah. The registered agent for service of process is CT Corporation System, 1108 E. South Union Ave., Midvale, UT 84047.

FACTUAL ALLEGATIONS

Defendants' Businesses

41. Landmark is a third-party administrator for insurance carriers.

42. Liberty Bankers is an insurance group that includes numerous affiliated companies, American Benefit Life Insurance Company, Liberty Bankers Life Insurance Company, and Capitol Life Insurance Company.

43. Accendo is a CVS Health Medicare supplement insurance provider offering Medicare Supplement Plans A, F, G, and N with varying amounts of coverage.

44. Plaintiffs and Class Members are current and former customers of Landmark's clients, including Liberty Bankers and Accendo.

45. In the course of their relationship, customers at Landmark's clients, including Plaintiffs and Class Members, provided Defendants with at least the following: names, driver's license numbers, tax identification numbers, and other sensitive information.

46. Upon information and belief, in the course of collecting Private Information from Plaintiffs and Class Members, Defendants promised to provide confidentiality and adequate security for the data it collected from them through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

47. Indeed, Liberty Bankers provides on its website that:

> We will take appropriate steps to protect all information you share with us. Whenever you provide the site with Personal Data, we will take commercially reasonable steps to establish a secure connection with your web browser.[3]

48. Accendo makes similar claims through the website belonging to Aetna, of which Accendo is a wholly owned subsidiary:

> Aetna considers personal information to be confidential and has policies and procedures in place to protect it against unlawful use and disclosure.[4]

49. Plaintiffs and the Class Members, as customers at Defendants' clients, including Liberty Bankers and Accendo, relied on these promises and relied on these sophisticated business entities to keep their sensitive Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Consumers, in general, demand security to safeguard their Private Information.

The Data Breach

50. On or about October 23, 2024, Landmark began sending Plaintiffs and other Data Breach victims a Notice of Data Breach letter (the "Notice Letter"), informing them that:

> **<u>What Happened</u>**
>
> On or about May 13, 2024, Landmark detected suspicious activity on its system. Upon discovery of this incident, Landmark

[3] https://www.lbig.com/privacy-policy
[4] https://www.aetnaseniorproducts.com/ssi/privacy_notice.html

> immediately disconnected the affected systems and remote access to the network and promptly engaged a specialized third-party cybersecurity firm and IT personnel to assist with securing the environment, as well as to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The forensic investigation concluded on or about July 24, 2024, and determined that there was unauthorized access to Landmark's network and data was encrypted and exfiltrated from its system. The unauthorized activity occurred from May 13, 2024 to June 17, 2024.
>
> Based on these findings, Landmark began reviewing the affected systems to identify the individuals potentially affected by this incident and the types of information that may have been compromised. While this process remains ongoing, and in an abundance of caution, Landmark is notifying potentially affected individuals by mail on a rolling basis as they are identified. We determined that some of your personal information may have been affected by the incident.
>
> **What Information Was Involved**
>
> The personal information that may have been subject to unauthorized access includes: name; tax identification number. For some individuals, it is possible that the following additional information may have been subject to unauthorized access (if this information was provided to Landmark): driver's license number; passport number; and medical and/or health information.[5]

51. Omitted from the Notice Letter were the identity of the cybercriminals who perpetrated this Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

52. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach's critical facts. Without

[5] The "Notice Letter". A sample copy is available at https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/2bd97a04-38be-40f1-94fd-9d143ea4bc9f.html

these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

53. Despite Landmark's intentional opacity about the root cause of this incident, several facts may be gleaned from the Notice Letter, including: a) that this Data Breach was the work of cybercriminals; b) that the cybercriminals first infiltrated Landmark's networks and systems, and downloaded data from the networks and systems; and c) that once inside Landmark's networks and systems, the cybercriminals targeted information, including Plaintiffs' and Class Members' Private Information, for download and theft.

54. In the context of notice of data breach letters of this type, Landmark's use of the phrase "may have been subject to unauthorized access" is misleading. Indeed, companies only send notice letters because data breach notification laws require them to do so under circumstances where there is a reasonable belief that such personal information was accessed or acquired by an unauthorized individual or entity. Thus, Landmark cannot hide behind legalese; by sending a notice of data breach letter to Plaintiffs and Class Members, it implicitly admits to having a reasonable belief that Plaintiffs' and Class Members' Private Information was accessed by unauthorized parties.

55. Moreover, in its Notice Letter, Landmark failed to specify whether it undertook any efforts to contact the approximate 1.6 million Class Members whose data was accessed and acquired in the Data Breach to inquire whether any of the Class Members suffered misuse of their data, whether Class Members should report their misuse to Landmark, and whether Landmark set up any mechanism for Class Members to report any misuse of their data.

56. Defendants had obligations created by the FTC Act, Gramm-Leach-Bliley Act, contract, common law, state statutes, and industry standards to keep Plaintiffs' and Class

Members' Private Information confidential and to protect it from unauthorized access and disclosure.

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

58. The attacker accessed and acquired files containing unencrypted Private Information of Plaintiffs and Class Members. Plaintiffs' and Class Members' Private Information was accessed and stolen in the Data Breach.

59. Some Plaintiffs have been informed by Experian and Credit Karma that their Private Information has been disseminated on the dark web, and Plaintiffs further believe that the Private Information 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.

Data Breaches Are Preventable

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

61. Defendants could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

62. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[6]

63. To prevent and detect cyber-attacks and/or ransomware attacks, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have written access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs,

[6] How to Protect Your Networks from RANSOMWARE, at 3, *available at:* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[7]

64. To prevent and detect cyber-attacks or ransomware attacks, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

> **Secure internet-facing assets**
>
> - Apply latest security updates
> - Use threat and vulnerability management
> - Perform regular audit; remove privileged credentials;
>
> **Thoroughly investigate and remediate alerts**
>
> - Prioritize and treat commodity malware infections as potential full compromise;
>
> **Include IT Pros in security discussions**
>
> - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
>
> **Build credential hygiene**
>
> - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;
>
> **Apply principle of least-privilege**
>
> - Monitor for adversarial activities
> - Hunt for brute force attempts

[7] *Id.* at 3-4.

- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[8]

65. Given that Landmark was storing the Private Information of its clients' current and former customers, Landmark could and should have implemented all of the above measures to prevent and detect cyberattacks.

66. The occurrence of the Data Breach indicates that Landmark failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and data thieves acquiring and accessing the Private Information of more than eight hundred thousand individuals, including that of Plaintiffs and Class Members.

Defendants Acquire, Collect & Store Plaintiffs' and the Class's Private Information

67. Landmark acquires, collects, and stores a massive amount of Private Information on its clients' current and former customers.

68. As a condition of obtaining services from Landmark and its clients, including Liberty Bankers and Accendo, individuals are required to entrust Landmark and its clients with highly sensitive personal information.

69. By obtaining, collecting, and using Plaintiffs' and Class Members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that

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

it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

70. Plaintiffs' and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and would not have entrusted it to Defendants absent a promise to safeguard that information.

71. Upon information and belief, in the course of collecting Private Information from Plaintiffs and Class Members, Defendants promised to provide confidentiality and adequate security for their data through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

72. Plaintiffs and the Class Members relied on Defendants to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Defendants Knew, Or Should Have Known, of the Risk of a Cyberattack Because Insurance Companies and Administrators in Possession of Private Information Are Particularly Susceptible To Such Attacks

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

74. Data breaches, including those perpetrated against insurance companies and administrators that store Private Information in their systems, have become widespread.

75. In 2023, an all-time high for data compromises occurred, with 3,205 compromises affecting 353,027,892 total victims. Of the 3,205 recorded data compromises, 809 of them, or 25.2% were in the medical or healthcare industry. The estimated number of organizations

impacted by data compromises has increased by +2,600 percentage points since 2018, and the estimated number of victims has increased by +1400 percentage points. The 2023 compromises represent a 78-percentage point increase over the previous year and a 72-percentage point hike from the previous all-time high number of compromises (1,860) set in 2021.

76. In light of recent high profile data breaches at other industry leading companies, including T-Mobile, USA (37 million records, February-March 2023), 23andMe, Inc. (20 million records, October 2023), Wilton Reassurance Company (1.4 million records, June 2023), NCB Management Services, Inc. (1 million records, February 2023), Defendants knew or should have known that the Private Information that they collected and maintained would be targeted by cybercriminals.

77. Indeed, cyber-attacks, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[9]

78. Additionally, as companies became more dependent on computer systems to run their business,[10] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[11]

[9] https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection

[10] https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html

[11] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022

79. Defendants knew and understood that unprotected or exposed Private Information in the custody of insurance administrators and companies is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Private Information through unauthorized access.

80. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendants' data security system were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

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

82. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

83. The ramifications of Defendants' failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen—particularly PHI—fraudulent use of that information and damage to victims may continue for years.

84. In the Notice Letter, Landmark makes an offer to provide identity monitoring services for a period of no longer than 24 months. This is wholly inadequate to compensate Plaintiffs and Class Members as it fail to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud,

and it entirely fail to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information.

85. Landmark's offer of credit and identity monitoring establishes that Plaintiffs' and Class Members' sensitive Private Information was in fact affected, accessed, compromised, and exfiltrated from Landmark's computer systems.

86. As an insurance company and administrator in custody of the Private Information of its clients' customers, Defendants knew, or should have known, the importance of safeguarding Private Information entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Defendants failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

Value of Personally Identifiable Information

87. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[12] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[13]

[12] 17 C.F.R. § 248.201 (2013).
[13] *Id.*

88. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[14]

89. For example, Personal Information can be sold at a price ranging from $40 to $200.[15] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[16]

90. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[17]

91. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (*e.g.,* patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the pharmaceutical industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

---

[14] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/

[15] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[16] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

[17] *Medical I.D. Theft*, EFraudPrevention. https://efraudprevention.net/home/education/?a=187#:~:text=A%20thief%20may%20use%20your,credit%20report%20may%20be%20affected. (last visited Nov. 6, 2023).

92. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[18] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[19] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[20]

93. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[21]

94. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[22]

95. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.[23] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[24]

---

[18] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/ (last accessed July 24, 2023).
[19] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed July 24, 2023).
[20] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches/ (last accessed July 24, 2023).
[21] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content (last accessed July 20, 2021)
[22] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last accessed July 24, 2023).
[23] *See* Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed July 24, 2023).
[24] *Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One,* EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-toknow-about-them-and-what-to-do-after-one/ (last accessed July 24, 2023).

96. Driver's license numbers, which were compromised in the Data Breach, are incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information."[25]

97. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1200 on the Dark Web. On its own, a forged license can sell for around $200."[26]

98. According to national credit bureau, Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.

99. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[27] However, this is not the case. As cybersecurity experts point out:

> "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that requires ID verification, or use the information to craft curated social engineering phishing attacks."[28]

---

[25] *Hackers Stole Customers' License Numbers From Geico In Months-Long Breach*, Forbes, Apr. 20, 2021, *available at:* https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658 (last visited July 31, 2023).

[26] https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658 (last visited on Feb. 21, 2023).

[27] https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/ (last visited on Feb. 21, 2023).

[28] *Id.*

100. Victims of driver's license number theft also often suffer unemployment benefit fraud, as described in a recent New York Times article.[29]

101. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—PHI and names.

102. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[30]

103. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

104. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years.

[29] *How Identity Thieves Took My Wife for a Ride,* NY Times, April 27, 2021, available at: https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html (last visited on Feb. 21, 2023).
[30] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

> As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[31]

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

Defendants Fail to Comply with FTC Guidelines

106. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

107. 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 consumer 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.[32]

108. 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.[33]

---

[31] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf.

[32] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

[33] *Id.*

109. 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 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.

110. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer 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.

111. These FTC enforcement actions include actions against insurance administrators and companies, like Defendants.

112. 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 Defendants, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

113. Defendants failed to properly implement basic data security practices.

114. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to the Private Information of its clients' customers 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.

115. Upon information and belief, Defendants were at all times fully aware of their obligation to protect the Private Information of Plaintiffs and Class Members and the significant repercussions that would result from their failure to do so. Accordingly, Defendants' conduct was particularly unreasonable given the nature and amount of Private Information they obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

Defendants Failed to Comply with the Gramm-Leach-Bliley Act

116. Defendants are financial institutions, as that term is defined by Section 509(3)(A) of the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6809(3)(A), and thus are subject to the GLBA.

117. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

118. Defendants collect nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n) and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period Defendants were subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1, *et seq*., and is subject to numerous rules and regulations promulgated on the GLBA statutes.

119. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the CFPB became responsible for implementing the Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

120. Accordingly, Defendants' conduct is governed by the Privacy Rule prior to December 30, 2011 and by Regulation P after that date.

121. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1). These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4 and 313.5; 12 C.F.R. §§ 1016.4 and 1016.5. They must include specified elements, including the categories of nonpublic personal information the financial institution collects and discloses, the categories of third parties to whom the financial institution discloses the information, and the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Defendants violated the Privacy Rule and Regulation P.

122. Upon information and belief, Defendants failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' Private Information and storing that Private Information on Landmark's network systems.

123. Defendants failed to adequately inform their customers that they were storing and/or sharing, or would store and/or share, the customers' Private Information on an insecure platform, accessible to unauthorized parties from the internet, and would do so after the customer relationship ended.

124. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3 and 314.4.

125. As alleged herein, Defendants violated the Safeguard Rule.

126. Defendants failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information and failed to monitor the systems of their IT partners or verify the integrity of those systems.

127. Defendants violated the GLBA and their own policies and procedures by sharing the Private Information of Plaintiffs and Class Members with a non-affiliated third party without providing Plaintiffs and Class Members (a) an opt-out notice, and (b) a reasonable opportunity to opt out of such disclosure.

Defendants Failed to Comply with Industry Standards

128. As noted above, experts studying cyber security routinely identify insurance administrators in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

129. Several best practices have been identified that, at a minimum, should be implemented by insurance administrators and companies in possession of Private Information, like Defendants, including but not limited to: 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. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

130. Other best cybersecurity practices that are standard for insurance administrators and companies 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; training staff regarding critical points. Defendants failed to follow these cybersecurity best practices, including failure to train staff.

131. Upon information and belief Defendants failed to meet the minimum standards of one or more of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's

Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

132. These foregoing frameworks are existing and applicable industry standards for insurance administrators and companies, and upon information and belief, Defendants failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

Common Injuries & Damages

133. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) uncompensated 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) nominal damages; and (viii) 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 Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

Data Breaches Increase Victims' Risk of Identity Theft

134. As some Plaintiffs have already experienced, the unencrypted Private Information of Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

135. 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 Plaintiffs and Class Members. Simply put, unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

136. 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.

137. Plaintiffs' 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 Plaintiffs and Class Members and to profit off their misfortune.

138. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[34]

139. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an

[34] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/

astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

140. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' 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 that was exfiltrated in the Data Breach, criminals may still 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.

141. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like contact information) of Plaintiffs and the other Class Members.

142. Thus, even if certain information (such as contact information) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

143. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

Loss of Time to Mitigate Risk of Identity Theft & Fraud

144. 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 – yet the resource and asset of time has been lost.

145. Thus, due to the actual and imminent risk of identity theft, Landmark, in its Notice Letter instructs Plaintiffs and Class Members to take the following measures to protect themselves: "remain vigilant and take steps to protect yourself against incidents of identity theft and fraud, including monitoring your accounts, account statements, and free credit reports for suspicious or unauthorized activity."[35]

146. In addition, Landmark's Notice letter includes multiple pages devoted to "Steps You Can Take To Help Protect Your Information" that recommend Plaintiffs and Class Members to partake in activities such as monitoring their accounts, placing security freezes and fraud alerts on their accounts, and contacting consumer reporting bureaus.[36]

147. Landmark's extensive suggestion of steps that Plaintiffs and Class Members must take in order to protect themselves from identity theft and/or fraud demonstrates the significant time that Plaintiffs and Class Members must undertake in response to the Data Breach. Plaintiffs' and Class Members' time is highly valuable and irreplaceable, and accordingly, Plaintiffs and Class Members suffered actual injury and damages in the form of uncompensated lost time that they spent on mitigation activities in response to the Data Breach and at the direction of Landmark's Notice Letter.

148. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach. Accordingly, the Data Breach has caused Plaintiffs and Class Members to suffer actual

[35] Notice Letter.
[36] *Id.*

injury in the form of uncompensated lost time—which cannot be recaptured—spent on mitigation activities.

149. Plaintiffs' 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."[37]

150. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider 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.[38]

151. 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."[4]

Diminution of Value of Private Information

152. PII and PHI are valuable property rights.[39] Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison

[37] *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.
[38] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps
[39] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf ("GAO Report").

sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

153. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[40]

154. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[41]

155. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[42,43]

156. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[44]

157. As a result of the Data Breach, Plaintiffs' 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 Plaintiffs 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.

158. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, and of the

[40] *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).
[41] *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/
[42] https://www.latimes.com/business/story/2019-11-05/column-data-brokers
[43] https://datacoup.com/
[44] https://digi.me/what-is-digime/

foreseeable consequences that would occur if Defendants' data security system were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

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

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

161. Landmark was, or should have been, fully aware of the unique type and the significant volume of data on Landmark's network, amounting to more than eight hundred thousand individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

162. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

163. Given the type of targeted attack in this case, sophisticated criminal activity, the type of Private Information involved, and Plaintiffs' Private Information already being disseminated on the dark web, 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.

164. 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.

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

166. 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 to protect Class Members from the risk of identity theft that arose from Defendants' Data Breach.

Loss of Benefit of the Bargain

167. Furthermore, Defendants' poor data security practices deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Landmark's clients, including Liberty Bankers, for products or services, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying for the product or service and necessary data security to protect the Private Information, when in fact, Landmark's did not provide the expected data security. Accordingly, Plaintiffs and Class Members received products or services that were of lesser value than what they reasonably expected to receive under the bargains they struck with Landmark's clients.

Plaintiffs' Experiences

Raymond Newson's Experience

168. Plaintiff Newson Private Information was entrusted to Liberty Bankers and Landmark in exchange for insurance services.

169. Plaintiff and Class members' Private Information was entrusted to Defendants Liberty Bankers and Landmark with the reasonable expectation and mutual understanding that they would keep such information confidential and secure from unauthorized access.

170. Plaintiff Newson received a notice letter from Landmark dated October 23, 2024, informing him that his Private Information was specifically identified as having been exposed to cybercriminals in the Data Breach.

171. Plaintiff Newson is very careful about sharing his sensitive information. To the best of Plaintiff's knowledge, he has never before had his Private Information exposed in any other data breach.

172. Plaintiff Newson stores any documents containing his Private Information in a safe and secure location. Plaintiff Newson has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

173. Because of the Data Breach, Plaintiff Newson's Private Information is now in the hands of cybercriminals.

174. Plaintiff Newson has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

175. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number, Plaintiff Newson is now imminently at risk of crippling future identity theft and fraud.

176. Since the Data Breach, Plaintiff Newson has experienced a noticeable increase in the number of spam calls he receives.

177. As a result of the Data Breach, Plaintiff Newson has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the

future consequences of the Breach. Among other things, Plaintiff Newson has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities and money-making opportunities.

178. The letter Plaintiff Newson received from Landmark specifically directed him to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised individuals affected by the breach to "remain vigilant and take steps to protect yourself against incidents of identity theft and fraud, including monitoring your accounts, account statements, and free credit reports for suspicious or unauthorized activity."[45] In addition, the breach notification advised that victims of the Data Breach should take Further steps to help protect themselves including: contacting their financial institution and major credit bureaus to inform them of the Data Breach and to follow any steps recommended, including the possible placement of a fraud alert on their credit file.[46]

179. As a result of the Data Breach, Plaintiff Newson has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Newson fears that criminals will use his information to commit identity theft.

[45] *See* sample breach notification letter, available at: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/2bd97a04-38be-40f1-94fd-9d143ea4bc9f.html

[46] *Id.*

180. Plaintiff Newson anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

181. Plaintiff Newson has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Newson's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Newson's Private Information that was entrusted to Defendants Liberty Bankers and Landmark; (d) damages unjustly retained by Defendants Liberty Bankers and Landmark at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendants Liberty Bankers and Landmark and their defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Newson's Private Information; and (e) continued risk to Plaintiff Newson's Private Information, which remains in the possession of Defendants Liberty Bankers and Landmark and which is subject to further breaches so long as they fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to them.

Plaintiff Britton Bryant's Experience

182. Plaintiff Bryant's Private Information was entrusted to Defendants Liberty Bankers and Landmark in exchange for insurance services.

183. Plaintiff and Class members' Private Information was entrusted to Defendants Liberty Bankers and Landmark with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

184. Plaintiff Bryant received a notice letter from Landmark dated October 23, 2024, informing him that his Private Information was specifically identified as having been exposed to cybercriminals in the Data Breach.

185. Plaintiff Bryant is very careful about sharing his sensitive information. To the best of Plaintiff's knowledge, he has never before had his Private Information exposed in any other data breach.

186. Plaintiff Bryant stores any documents containing his Private Information in a safe and secure location. Plaintiff Bryant has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

187. Because of the Data Breach, Plaintiff Bryant's Private Information is now in the hands of cybercriminals.

188. Plaintiff Bryant has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

189. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number, Plaintiff Bryant is now imminently at risk of crippling future identity theft and fraud.

190. Since the Data Breach, Plaintiff Bryant has experienced identity theft in the form of fraudulent charges on his financial account. Plaintiff Bryant attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that he has never experienced anything like this prior to now, and the fact that he is very careful with his Private Information.

191. As a result of the Data Breach, Plaintiff Bryant has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the

future consequences of the Breach. Among other things, Plaintiff Bryant has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and credit reports, enrolling in credit monitoring services, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities and money-making opportunities.

192. The letter Plaintiff Bryant received from Landmark specifically directed him to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised individuals affected by the breach to "remain vigilant and take steps to protect yourself against incidents of identity theft and fraud, including monitoring your accounts, account statements, and free credit reports for suspicious or unauthorized activity." In addition, the breach notification advised that victims of the Data Breach should take Further steps to help protect themselves including: contacting their financial institution and major credit bureaus to inform them of the Data Breach and to follow any steps recommended, including the possible placement of a fraud alert on their credit file.

193. As a result of the Data Breach, Plaintiff Bryant has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Bryant fears that criminals will use his information to commit identity theft.

194. Plaintiff Bryant anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

195. Plaintiff Bryant has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Bryant's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Bryant's Private Information that was entrusted to Defendants Liberty Bankers and Landmark; (d) damages unjustly retained by Defendants Liberty Bankers and Landmark at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendants and Defendants' defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Bryant's Private Information; and (e) continued risk to Plaintiff Bryant's Private Information, which remains in the possession of Defendants Liberty Bankers and Landmark and which is subject to further breaches so long as they fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to them.

Plaintiff Donald Tanner's Experience

196. Plaintiff Tanner's Private Information was entrusted to Defendants Liberty Bankers and Landmark in exchange for insurance services.

197. Plaintiff and Class members' Private Information was entrusted to Defendants Liberty Bankers and Landmark with the reasonable expectation and mutual understanding that Defendants would keep such information confidential and secure from unauthorized access.

198. Plaintiff Tanner received a notice letter from Landmark dated October 23, 2024, informing him that his Private Information was specifically identified as having been exposed to cybercriminals in the Data Breach.

199. Plaintiff Tanner is very careful about sharing his sensitive information. To the best of Plaintiff's knowledge, he has never before had his Private Information exposed in any other data breach.

200. Plaintiff Tanner stores all documents containing his Private Information in a safe and secure location. Plaintiff Tanner has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

201. Because of the Data Breach, Plaintiff Tanner's Private Information is now in the hands of cybercriminals.

202. Plaintiff Tanner has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

203. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number, Plaintiff Tanner is now imminently at risk of crippling future identity theft and fraud.

204. Since the Data Breach, Plaintiff Tanner has experienced identity theft. For example, in August 2024, unknown individuals attempted to fraudulently remove funds from Plaintiff Tanner's personal bank account. Since the Data Breach, Plaintiff Tanner has also received notices stating he owed money for bills he did not recognize. Further, in the fall of 2024, Plaintiff Tanner received notifications that his Private Information has been posted to the dark web. Plaintiff Tanner attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that he is very careful with his Private Information, and the fact that he has never experienced anything like this prior to now.

205. As a result of the Data Breach, Plaintiff Tanner has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the

future consequences of the Breach. Among other things, Plaintiff Tanner has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and credit reports, enrolling in credit monitoring services, contacting his bank regarding fraudulent activity, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities and money-making opportunities.

206. The letter Plaintiff Tanner received from Landmark specifically directed him to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised individuals affected by the breach to "remain vigilant and take steps to protect yourself against incidents of identity theft and fraud, including monitoring your accounts, account statements, and free credit reports for suspicious or unauthorized activity."

207. In addition, the breach notification advised that victims of the Data Breach should take Further steps to help protect themselves including: contacting their financial institution and major credit bureaus to inform them of the Data Breach and to follow any steps recommended, including the possible placement of a fraud alert on their credit file.

208. As a result of the Data Breach, Plaintiff Tanner has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Tanner fears that criminals will use his information to commit identity theft.

209. Plaintiff Tanner anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

210. Plaintiff Tanner has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Tanner's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Tanner's Private Information that was entrusted to Defendants Liberty Bankers and Landmark; (d) damages unjustly retained by Defendants Liberty Bankers and Landmark at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendants and Defendants' defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Tanner's Private Information; and (e) continued risk to Plaintiff Tanner's Private Information, which remains in the possession of Defendants Liberty Bankers and Landmark and which is subject to further breaches so long as they fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to them.

Plaintiff Edna Whitten's Experience

211. Plaintiff Whitten Private Information was entrusted to Defendants Liberty Bankers and Landmark in exchange for insurance services.

212. Plaintiff and Class members' Private Information was entrusted to Defendants Liberty Bankers and Landmark with the reasonable expectation and mutual understanding that they would keep such information confidential and secure from unauthorized access.

213. Plaintiff Whitten received a notice letter from Landmark dated October 23, 2024, informing her that her Private Information was specifically identified as having been exposed to cybercriminals in the Data Breach.

214. Plaintiff Whitten is very careful about sharing her sensitive information. To the best of Plaintiff's knowledge, she has never before had her Private Information exposed in any other data breach.

215. Plaintiff Whitten stores any documents containing her Private Information in a safe and secure location. Plaintiff Whitten has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

216. Because of the Data Breach, Plaintiff Whitten's Private Information is now in the hands of cybercriminals.

217. Plaintiff Whitten has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

218. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number, Plaintiff Whitten is now imminently at risk of crippling future identity theft and fraud.

219. Since the Data Breach, Plaintiff has received notifications advising her that her Private Information has been posted to the dark web. In addition, in the months since the Data Breach, Plaintiff Whitten has experienced a noticeable increase in the volume of spam text messages she receives. Many of these messages relate to a mortgage on a home she has already paid off. Plaintiff Whitten attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, and the fact that she has never experienced anything like this prior to now.

220. As a result of the Data Breach, Plaintiff Whitten has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Whitten has already expended

time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, screening spam calls, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities and money-making opportunities.

221. The letter Plaintiff Whitten received from Landmark specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised individuals affected by the breach to "remain vigilant and take steps to protect yourself against incidents of identity theft and fraud, including monitoring your accounts, account statements, and free credit reports for suspicious or unauthorized activity." In addition, the breach notification advised that victims of the Data Breach should take further steps to help protect themselves including: contacting their financial institution and major credit bureaus to inform them of the Data Breach and to follow any steps recommended, including the possible placement of a fraud alert on their credit file.

222. As a result of the Data Breach, Plaintiff Whitten has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Whitten fears that criminals will use her information to commit identity theft.

223. Plaintiff Whitten anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

224. Plaintiff Whitten has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and

certainly impending injury flowing from fraud and identity theft posed by Plaintiff Whitten's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Whitten's Private Information that was entrusted to Defendants Liberty Bankers and Landmark; (d) damages unjustly retained by Defendants Liberty Bankers and Landmark at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendants and Defendants' defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Whitten's Private Information; and (e) continued risk to Plaintiff Whitten's Private Information, which remains in the possession of Defendants Liberty Bankers and Landmark and which is subject to further breaches so long as they fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to them.

Plaintiff Folayan Payne's Experience

225. Plaintiff Payne Private Information was entrusted to Defendants Liberty Bankers and Landmark in exchange for insurance services.

226. Plaintiff and Class members' Private Information was entrusted to Defendants Liberty Bankers and Landmark with the reasonable expectation and mutual understanding that they would keep such information confidential and secure from unauthorized access.

227. Plaintiff Payne received a notice letter from Landmark dated October 23, 2024, informing him that his Private Information was specifically identified as having been exposed to cybercriminals in the Data Breach.

228. Plaintiff Payne is very careful about sharing his sensitive information. To the best of Plaintiff's knowledge, he has never before had his Private Information exposed in any other data breach.

229. Plaintiff Payne stores any documents containing his Private Information in a safe and secure location. Plaintiff Payne has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

230. Because of the Data Breach, Plaintiff Payne's Private Information is now in the hands of cybercriminals.

231. Plaintiff Payne has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

232. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number, Plaintiff Payne is now imminently at risk of crippling future identity theft and fraud.

233. Since the Data Breach, Plaintiff Payne has experienced a noticeable increase in the number of spam phone calls he receives on a daily basis.

234. As a result of the Data Breach, Plaintiff Payne has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Payne has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, researching and enrolling in credit monitoring, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities and money-making opportunities.

235. The letter Plaintiff Payne received from Landmark specifically directed him to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all

Class Members advised individuals affected by the breach to "remain vigilant and take steps to protect yourself against incidents of identity theft and fraud, including monitoring your accounts, account statements, and free credit reports for suspicious or unauthorized activity."[47] In addition, the breach notification advised that victims of the Data Breach should take Further steps to help protect themselves including: contacting their financial institution and major credit bureaus to inform them of the Data Breach and to follow any steps recommended, including the possible placement of a fraud alert on their credit file.[48]

236. As a result of the Data Breach, Plaintiff Payne has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Payne fears that criminals will use his information to commit identity theft.

237. Plaintiff Payne anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

238. Plaintiff Payne has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Payne's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Payne's Private Information that was entrusted to Defendants Liberty Bankers and Landmark; (d) damages unjustly retained by Defendants Liberty Bankers and Landmark at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from

[47] *See* sample breach notification letter, available at: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/2bd97a04-38be-40f1-94fd-9d143ea4bc9f.html

[48] *Id.*

Defendants and Defendants' defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Payne's Private Information; and (e) continued risk to Plaintiff Payne's Private Information, which remains in the possession of Defendants Liberty Bankers and Landmark and which is subject to further breaches so long as they fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to them.

Plaintiff Drenetha Goff's Experience

239. Plaintiff Goff Private Information was entrusted to Accendo and Landmark in exchange for insurance services.

240. Plaintiff and Class Members' Private Information was entrusted to Defendants, Accendo and Landmark, with the reasonable expectation and mutual understanding that Defendants would keep such information confidential and secure from unauthorized access.

241. Plaintiff Goff received a notice letter from Landmark dated January 22, 2025, informing her that her Private Information was specifically identified as having been exposed to cybercriminals in the Data Breach.

242. Plaintiff Goff is very careful about sharing her sensitive information.

243. Plaintiff Goff stores any documents containing her Private Information in a safe and secure location. Plaintiff Goff has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

244. Because of the Data Breach, Plaintiff Goff's Private Information is now in the hands of cybercriminals.

245. Plaintiff Goff has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

246. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number, Plaintiff Goff is now imminently at risk of crippling future identity theft and fraud.

247. Since the Data Breach, Plaintiff Goff has experienced identity theft. Specifically, in early 2025, Plaintiff Goff was notified of a credit card fraudulently applied for in her name. Further, in the months since the Data Breach, Plaintiff Goff has experienced a noticeable increase in spam text messages and emails. Plaintiff Goff attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that she is very careful with her Private Information, and the fact that nothing like this had ever happened to her before.

248. As a result of the Data Breach, Plaintiff Goff has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Goff has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities and money-making opportunities.

249. The letter Plaintiff Goff received from Defendants specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised individuals affected by the breach to "remain vigilant and take steps to protect yourself against incidents of identity theft and fraud, including monitoring your accounts, account statements, and free credit reports for suspicious or unauthorized activity." In addition, the breach notification advised that victims of the Data Breach should take further steps to help

protect themselves including: contacting their financial institution and major credit bureaus to inform them of the Data Breach and to follow any steps recommended, including the possible placement of a fraud alert on their credit file.

250. As a result of the Data Breach, Plaintiff Goff has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Goff fears that criminals will use her information to commit identity theft.

251. Plaintiff Goff anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

252. Plaintiff Goff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Goff's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Goff's Private Information that was entrusted to Defendants Accendo and Landmark; (d) damages unjustly retained by Defendants Accendo and Landmark at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendants Accendo and Landmark and their defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Goff's Private Information; and (e) continued risk to Plaintiff Goff's Private Information, which remains in the possession of Defendants Accendo and Landmark and which is subject to further breaches so long as they fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to them.

Plaintiff Kara Montague's Experience

253. Plaintiff Montague Private Information was entrusted to Liberty Bankers and Landmark in exchange for insurance services.

254. Plaintiff and Class members' Private Information was entrusted to Defendants Liberty Bankers and Landmark with the reasonable expectation and mutual understanding that they would keep such information confidential and secure from unauthorized access.

255. Plaintiff Montague received a notice letter from Landmark dated October 23, 2024, informing her that her Private Information was specifically identified as having been exposed to cybercriminals in the Data Breach.

256. Plaintiff Montague is very careful about sharing her sensitive information.

257. Plaintiff Montague stores any documents containing her Private Information in a safe and secure location. Plaintiff Montague has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

258. Because of the Data Breach, Plaintiff Montague's Private Information is now in the hands of cybercriminals.

259. Plaintiff Montague has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

260. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number, Plaintiff Montague is now imminently at risk of crippling future identity theft and fraud.

261. Since the Data Breach, Plaintiff Montague has experienced identity theft. Specifically, in October 2024, Plaintiff Montague experienced an authorized and fraudulent transaction on her financial account. In addition, following the Data Breach. Plaintiff Montague has received notifications that her Private Information has been located on the dark web. Further,

in the months since the Data Breach, Plaintiff Montague has experienced a noticeable increase in spam text messages and emails. Plaintiff Montague attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity.

262. As a result of the Data Breach, Plaintiff Montague has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Montague has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, signing up for and monitoring her dark web monitoring service, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities and money-making opportunities.

263. The letter Plaintiff Montague received from Landmark specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised individuals affected by the breach to "remain vigilant and take steps to protect yourself against incidents of identity theft and fraud, including monitoring your accounts, account statements, and free credit reports for suspicious or unauthorized activity."[49] In addition, the breach notification advised that victims of the Data Breach should take further steps to help protect themselves including: contacting their financial institution and major credit bureaus to

[49] *See* sample breach notification letter, available at: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/2bd97a04-38be-40f1-94fd-9d143ea4bc9f.html

inform them of the Data Breach and to follow any steps recommended, including the possible placement of a fraud alert on their credit file.[50]

264. As a result of the Data Breach, Plaintiff Montague has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Montague fears that criminals will use her information to commit identity theft.

265. Plaintiff Montague anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

266. Plaintiff Montague has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Montague's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Montague's Private Information that was entrusted to Defendants Liberty Bankers and Landmark; (d) damages unjustly retained by Defendants Liberty Bankers and Landmark at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendants Liberty Bankers and Landmark and their defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Montague's Private Information; and (e) continued risk to Plaintiff Montague's Private Information, which remains in the possession of Defendants Liberty Bankers and Landmark and which is subject to further breaches so long as they fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to them.

Plaintiff Karina Barratt

[50] *Id.*

267. Plaintiff Barratt Private Information was entrusted to Liberty Bankers and Landmark in exchange for insurance services.

268. Plaintiff and Class members' Private Information was entrusted to Defendants Liberty Bankers and Landmark with the reasonable expectation and mutual understanding that they would keep such information confidential and secure from unauthorized access.

269. Plaintiff Barratt received a notice letter from Landmark dated October 23, 2024, informing her that her Private Information was specifically identified as having been exposed to cybercriminals in the Data Breach.

270. Plaintiff Barratt is very careful about sharing her sensitive information.

271. Plaintiff Barratt stores any documents containing her Private Information in a safe and secure location. Plaintiff Barratt has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

272. Because of the Data Breach, Plaintiff Barratt's Private Information is now in the hands of cybercriminals.

273. Plaintiff Barratt has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

274. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number, Plaintiff Barratt is now imminently at risk of crippling future identity theft and fraud.

275. Since the Data Breach, Plaintiff Barratt has experienced identity theft. Specifically, in August of 2024, Plaintiff Barratt was advised of an unauthorized and fraudulent mortgage that was opened in her name. In addition, in August 2024 and in November 2024, Plaintiff Barratt experienced unauthorized transactions on her financial accounts. Further, since the Data Breach,

Plaintiff Barratt has received an increased volume of spam text messages and phone calls, requiring her to change ger phone number twice since the time of the Data Breach. Plaintiff Barratt has also received notifications from the credit monitoring services Experian and IDX that her Private Information was located on the dark web. Plaintiff Barratt attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, and the fact that she has never experienced anything like this prior to now.

276. As a result of the Data Breach, Plaintiff Barratt has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Barratt has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, placing a freeze on her credit accounts, signing up for credit monitoring, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities and money-making opportunities.

277. The letter Plaintiff Barratt received from Landmark specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised individuals affected by the breach to "remain vigilant and take steps to protect yourself against incidents of identity theft and fraud, including monitoring your accounts, account statements, and free credit reports for suspicious or unauthorized activity."[51] In addition, the breach notification advised that victims of the Data Breach should take further steps to help

[51] *See* sample breach notification letter, available at: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/2bd97a04-38be-40f1-94fd-9d143ea4bc9f.html

protect themselves including: contacting their financial institution and major credit bureaus to inform them of the Data Breach and to follow any steps recommended, including the possible placement of a fraud alert on their credit file.[52]

278. As a result of the Data Breach, Plaintiff Barratt has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Barratt fears that criminals will use her information to commit identity theft.

279. Plaintiff Barratt anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

280. Plaintiff Barratt has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Barratt's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Barratt's Private Information that was entrusted to Defendants Liberty Bankers and Landmark; (d) damages unjustly retained by Defendants Liberty Bankers and Landmark at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendants Liberty Bankers and Landmark and their defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Barratt's Private Information; and (e) continued risk to Plaintiff Barratt's Private Information, which remains in the possession of Defendants Liberty Bankers and Landmark and which is subject to further breaches so long as they fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to them.

[52] *Id*.

Plaintiff Lynda Roberts Experience

281. Plaintiff Roberts Private Information was entrusted to Liberty Bankers and Landmark in exchange for insurance services.

282. Plaintiff and Class members' Private Information was entrusted to Defendants Liberty Bankers and Landmark with the reasonable expectation and mutual understanding that they would keep such information confidential and secure from unauthorized access.

283. Plaintiff Roberts received a notice letter from Landmark dated October 23, 2024, informing her that her Private Information was specifically identified as having been exposed to cybercriminals in the Data Breach.

284. Plaintiff Roberts is very careful about sharing her sensitive information. The Plaintiff's Private Information has previously been exposed in a data breach involving AT&T. Plaintiff did not experience any identity theft or related harms as a result of the prior incident.

285. Plaintiff Roberts stores any documents containing her Private Information in a safe and secure location. Plaintiff Roberts has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

286. Because of the Data Breach, Plaintiff Roberts's Private Information is now in the hands of cybercriminals.

287. Plaintiff Roberts has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

288. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number, Plaintiff Roberts is now imminently at risk of crippling future identity theft and fraud.

289. Since the Data Breach, Plaintiff Roberts has experienced data misuse in the form of her Experian credit report being linked to an unrecognized Social Security number. Further, in the months following the Data Breach, Plaintiff Roberts has experienced a notable increase in the number of spam phone calls received. Plaintiff Roberts attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, and the fact that she has never experienced anything like this prior to now.

290. As a result of the Data Breach, Plaintiff Roberts has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Roberts has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities and money-making opportunities.

291. The letter Plaintiff Roberts received from Landmark specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised individuals affected by the breach to "remain vigilant and take steps to protect yourself against incidents of identity theft and fraud, including monitoring your accounts, account statements, and free credit reports for suspicious or unauthorized activity."[53] In addition, the breach notification advised that victims of the Data Breach should take further steps to help protect themselves including: contacting their financial institution and major credit bureaus to

[53] *See* sample breach notification letter, available at: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/2bd97a04-38be-40f1-94fd-9d143ea4bc9f.html

inform them of the Data Breach and to follow any steps recommended, including the possible placement of a fraud alert on their credit file.[54]

292. As a result of the Data Breach, Plaintiff Roberts has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Roberts fears that criminals will use her information to commit identity theft.

293. Plaintiff Roberts anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

294. Plaintiff Roberts has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Roberts's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Roberts's Private Information that was entrusted to Defendants Liberty Bankers and Landmark; (d) damages unjustly retained by Defendants Liberty Bankers and Landmark at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendants Liberty Bankers and Landmark and their defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Roberts's Private Information; and (e) continued risk to Plaintiff Roberts's Private Information, which remains in the possession of Defendants Liberty Bankers and Landmark and which is subject to further breaches so long as they fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to them.

Plaintiff Randy Jackson's Experience

[54] *Id.*

295. Plaintiff Jackson Private Information was entrusted to Liberty Bankers and Landmark in exchange for insurance services.

296. Plaintiff and Class members' Private Information was entrusted to Defendants Liberty Bankers and Landmark with the reasonable expectation and mutual understanding that they would keep such information confidential and secure from unauthorized access.

297. Plaintiff Jackson received a notice letter from Landmark dated October 2Jackson, 2024, informing him that his Private Information was specifically identified as having been exposed to cybercriminals in the Data Breach.

298. Plaintiff Jackson is very careful about sharing his sensitive information. To the best of Plaintiff's knowledge, he has never before had his Private Information exposed in any other data breach.

299. Plaintiff Jackson stores any documents containing his Private Information in a safe and secure location. Plaintiff Jackson has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

300. Because of the Data Breach, Plaintiff Jackson's Private Information is now in the hands of cybercriminals.

301. Plaintiff Jackson has suffered actual injury from the exposure and theft of his Private Information—which violates his right to privacy.

302. As a result of the Data Breach, which exposed highly valuable information such as his Social Security number, Plaintiff Jackson is now imminently at risk of crippling future identity theft and fraud.

303. As a result of the Data Breach, Plaintiff Jackson has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the

future consequences of the Breach. Among other things, Plaintiff Jackson has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities and money-making opportunities.

304. The letter Plaintiff Jackson received from Landmark specifically directed him to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised individuals affected by the breach to "remain vigilant and take steps to protect yourself against incidents of identity theft and fraud, including monitoring your accounts, account statements, and free credit reports for suspicious or unauthorized activity."[55] In addition, the breach notification advised that victims of the Data Breach should take further steps to help protect themselves including: contacting their financial institution and major credit bureaus to inform them of the Data Breach and to follow any steps recommended, including the possible placement of a fraud alert on their credit file.[56]

305. As a result of the Data Breach, Plaintiff Jackson has experienced stress, anxiety, and concern due to the loss of his privacy and concern over the impact of cybercriminals accessing and misusing his Private Information. Plaintiff Jackson fears that criminals will use his information to commit identity theft.

[55] *See* sample breach notification letter, available at: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/2bd97a04-38be-40f1-94fd-9d143ea4bc9f.html

[56] *Id.*

306. Plaintiff Jackson anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

307. Plaintiff Jackson has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Jackson's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Jackson's Private Information that was entrusted to Defendants Liberty Bankers and Landmark; (d) damages unjustly retained by Defendants Liberty Bankers and Landmark at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendants Liberty Bankers and Landmark and their defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Jackson's Private Information; and (e) continued risk to Plaintiff Jackson's Private Information, which remains in the possession of Defendants Liberty Bankers and Landmark and which is subject to further breaches so long as they fail to undertake appropriate and adequate measures to protect the Private Information that was entrusted to them.

Plaintiff Rozalynn Fisher's Experience

308. Plaintiff Fisher's Private Information was entrusted to Landmark in exchange for insurance services.

309. Plaintiff and Class members' Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

310. Plaintiff Fisher received a notice letter from Defendant dated October 23, 2024, informing her that her Private Information was specifically identified as having been exposed to cybercriminals in the Data Breach.

311. Plaintiff Fisher is very careful about sharing her sensitive information. To the best of her knowledge, Plaintiff has not previously had her Private Information exposed in a prior data breach.

312. Plaintiff Fisher stores any documents containing her Private Information in a safe and secure location. Plaintiff Fisher has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

313. Because of the Data Breach, Plaintiff Fisher's Private Information is now in the hands of cybercriminals.

314. Plaintiff Fisher has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

315. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number, Plaintiff Fisher is now imminently at risk of crippling future identity theft and fraud.

316. Since the Data Breach, Plaintiff Fisher has experienced identity theft in the form of unknown individuals attempting to take out credit cards and loans in her name. These attempts have had a negative impact on Plaintiff's credit. Plaintiff Fisher attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity, the fact that she is very careful with her Private Information, and the fact that nothing like this has ever happened to her before.

317. As a result of the Data Breach, Plaintiff Fisher has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Fisher has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing all account statements and other information, updating auto-payment information and passwords on impacted accounts, addressing the identity theft she has experienced, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities and money-making opportunities.

318. The letter Plaintiff Fisher received from Defendant specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised individuals affected by the breach to "remain vigilant and take steps to protect yourself against incidents of identity theft and fraud, including monitoring your accounts, account statements, and free credit reports for suspicious or unauthorized activity."[57] In addition, the breach notification advised that victims of the Data Breach should take further steps to help protect themselves including: contacting their financial institution and major credit bureaus to inform them of the Data Breach and to follow any steps recommended, including the possible placement of a fraud alert on their credit file.[58]

[57] *See* sample breach notification letter, available at: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/2bd97a04-38be-40f1-94fd-9d143ea4bc9f.html

[58] *Id.*

319. As a result of the Data Breach, Plaintiff Fisher has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Fisher fears that criminals will use her information to commit identity theft.

320. Plaintiff Fisher anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

321. Plaintiff Fisher has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Fisher's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Fisher's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Fisher's Private Information; and (e) continued risk to Plaintiff Fisher's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Shalene Willis's Experience

322. Plaintiff Willis' Private Information was entrusted to Landmark in exchange for insurance services.

323. Plaintiff and Class members' Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

324. Plaintiff Willis received a notice letter from Defendant dated October 23, 2024, informing her that her Private Information was specifically identified as having been exposed to cybercriminals in the Data Breach.

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

326. Because of the Data Breach, Plaintiff Willis's Private Information is now in the hands of cybercriminals.

327. Plaintiff Willis has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

328. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number, Plaintiff Willis is now imminently at risk of crippling future identity theft and fraud.

329. Since the Data Breach, Plaintiff Willis has experienced identity theft in the form of unknown individuals attempting to make purchases at Home Depot and Apple using her information without authorization. Further, following the Data Breach, Plaintiff has received notice from CreditKarma (a credit monitoring service) that her Private Information has been posted to the dark web. Plaintiff Willis attributes the foregoing suspicious and unauthorized activity to the Data Breach given the time proximity.

330. As a result of the Data Breach, Plaintiff Willis has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Willis has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts about the Data Breach, thoroughly reviewing account statements and other information, reconciling fraud attempts, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities and money-making opportunities.

331. The letter Plaintiff Willis received from Defendant specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised individuals affected by the breach to "remain vigilant and take steps to protect yourself against incidents of identity theft and fraud, including monitoring your accounts, account statements, and free credit reports for suspicious or unauthorized activity."[59] In addition, the breach notification advised that victims of the Data Breach should take further steps to help protect themselves including: contacting their financial institution and major credit bureaus to inform them of the Data Breach and to follow any steps recommended, including the possible placement of a fraud alert on their credit file.[60]

332. As a result of the Data Breach, Plaintiff Willis has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing

[59] *See* sample breach notification letter, available at: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/2bd97a04-38be-40f1-94fd-9d143ea4bc9f.html

[60] *Id.*

and misusing her Private Information. Plaintiff Willis fears that criminals will use her information to commit identity theft.

333. Plaintiff Willis anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

334. Plaintiff Willis has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certainly impending injury flowing from fraud and identity theft posed by Plaintiff Willis's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Willis's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Willis's Private Information; and (e) continued risk to Plaintiff Willis's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Sharika Dodson's Experience

335. Plaintiff Dodson Private Information was entrusted to Landmark in exchange for insurance services.

336. Plaintiff and Class members' Private Information was entrusted to Defendant with the reasonable expectation and mutual understanding that Defendant would keep such information confidential and secure from unauthorized access.

337. Plaintiff Dodson received a notice letter from Defendant dated October 23, 2024, informing her that her Private Information was specifically identified as having been exposed to cybercriminals in the Data Breach.

338. Plaintiff Dodson is very careful about sharing her sensitive information. To the best of Plaintiff's knowledge, she has never before had her Private Information exposed in any other data breach.

339. Plaintiff Dodson stores any documents containing her Private Information in a safe and secure location. Plaintiff Dodson has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

340. Because of the Data Breach, Plaintiff Dodson's Private Information is now in the hands of cybercriminals.

341. Plaintiff Dodson has suffered actual injury from the exposure and theft of her Private Information—which violates her right to privacy.

342. As a result of the Data Breach, which exposed highly valuable information such as her Social Security number, Plaintiff Dodson is now imminently at risk of crippling future identity theft and fraud.

343. Since the Data Breach, Plaintiff Dodson has experienced a notable increase in the number of spam calls she receives.

344. As a result of the Data Breach, Plaintiff Dodson has had no choice but to spend numerous hours attempting to mitigate the harms caused by the Data Breach and addressing the future consequences of the Breach. Among other things, Plaintiff Dodson has already expended time and suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including researching facts

about the Data Breach, thoroughly reviewing account statements and other information, and taking other protective and ameliorative steps in response to the Data Breach. This is time that was lost and unproductive and took away from other activities and money-making opportunities.

345. The letter Plaintiff Dodson received from Defendant specifically directed her to take the actions described above. Indeed, the breach notification letter addressed to Plaintiff and all Class Members advised individuals affected by the breach to "remain vigilant and take steps to protect yourself against incidents of identity theft and fraud, including monitoring your accounts, account statements, and free credit reports for suspicious or unauthorized activity."[61] In addition, the breach notification advised that victims of the Data Breach should take further steps to help protect themselves including: contacting their financial institution and major credit bureaus to inform them of the Data Breach and to follow any steps recommended, including the possible placement of a fraud alert on their credit file.[62]

346. As a result of the Data Breach, Plaintiff Dodson has experienced stress, anxiety, and concern due to the loss of her privacy and concern over the impact of cybercriminals accessing and misusing her Private Information. Plaintiff Dodson fears that criminals will use her information to commit identity theft.

347. Plaintiff Dodson anticipates spending considerable time and money on an ongoing basis to remedy the harms caused by the Data Breach.

348. Plaintiff Dodson has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and

[61] *See* sample breach notification letter, available at: https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/2bd97a04-38be-40f1-94fd-9d143ea4bc9f.html

[62] *Id.*

certainly impending injury flowing from fraud and identity theft posed by Plaintiff Dodson's Private Information being placed in the hands of cybercriminals; (c) damages to and/or diminution in value of Plaintiff Dodson's Private Information that was entrusted to Defendant; (d) damages unjustly retained by Defendant at the cost to Plaintiff, including the difference in value between what Plaintiff should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security to protect Plaintiff Dodson's Private Information; and (e) continued risk to Plaintiff Dodson's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

CLASS ALLEGATIONS

349. Pursuant to Rule 42 of the Texas Rules of Civil Procedure, Plaintiffs propose the following Classes definitions, subject to amendment as appropriate:

350. The Classes that Plaintiffs seek to represent is defined as follows:

> **Nationwide Class**
> All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach reported by Landmark in October 2024 (the "Nationwide Class").

351. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants have 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.

352. Plaintiffs reserve the right to amend the definitions of the Classes or add additional Classes or Subclasses if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

353. Numerosity: The members of the Classes are so numerous that joinder of all members is impracticable, if not completely impossible. Indeed, at least 1.6 million Class Members were impacted in the Data Breach. The Classes are apparently identifiable within Defendants' records, and Landmark has already identified these individuals (as evidenced by sending them breach notification letters).

354. Common questions of law and fact exist as to all members of the Classes and predominate over any questions affecting solely individual members of the Classes. Among the questions of law and fact common to the Classes that predominate over questions which may affect individual Class members, including the following:

a. Whether and to what extent Defendants had a duty to protect the Private Information of Plaintiffs and Class Members;
b. Whether Defendants had respective duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;
c. Whether Defendants had respective duties not to use the Private Information of Plaintiffs and Class Members for non-business purposes;
d. Whether Defendants failed to adequately safeguard the Private Information of Plaintiffs and Class Members;
e. Whether and when Defendants actually learned of the Data Breach;
f. Whether Defendants adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;

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

h. Whether Defendants 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 Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Plaintiffs and Class Members are entitled to actual damages and/or nominal damages as a result of Defendants' wrongful conduct;

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

355. Typicality: Plaintiffs' claims are typical of those of the other members of the Class because Plaintiffs, like every other Class Member, were exposed to virtually identical conduct and now suffer from the same violations of the law as each other member of the Class.

356. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendants acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

357. Adequacy: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that would be antagonistic

to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

358. Superiority and Manageability: The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

359. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause

of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

360. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrate that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

361. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

362. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the Private Information of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Petition.

363. Further, Defendants have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

364. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants failed to timely notify the Plaintiffs and the class of the Data Breach;

b. Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendants' security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendants failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

365. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein, and brings this claim against all Defendants.

366. Landmark requires its clients' customers, including Plaintiffs and Class Members, to submit non-public Private Information in the ordinary course of providing services. As such, Defendants each gathered and stored the Private Information of Plaintiffs and Class Members as part of their business operations.

367. Plaintiffs and Class Members entrusted Defendants with their Private Information with the understanding that Defendants would safeguard it.

368. Defendants had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed.

369. By voluntarily undertaking and assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants 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. Defendants' duty included a responsibility to implement processes by which they could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

370. Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

371. Defendants' duty to use reasonable security measures also arose under the GLBA, under which they were required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards.

372. Defendants owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks adequately protected the Private Information.

373. Defendants' duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and the Class entrusted Defendants with their confidential Private Information, a necessary part of being customers at Landmark's clients, including Liberty Bankers.

374. Defendants' 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 Defendants are bound by industry standards to protect confidential Private Information.

375. Defendants were subject to an "independent duty," untethered to any contract between Defendants and Plaintiffs or the Class.

376. Defendants also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain pursuant to regulations.

377. Moreover, Defendants had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

378. Defendants had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and the Class within Defendants' possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

379. Defendants breached their duties, pursuant to the FTC Act, GLBA, and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

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;

c. Allowing unauthorized access to Class Members' Private Information;

d. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

e. Failing to remove former customers' Private Information it was no longer required to retain pursuant to regulations, and

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

380. Defendants violated Section 5 of the FTC Act and GLBA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendants' 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 Plaintiffs and the Class.

381. Plaintiffs and Class Members were within the class of persons the Federal Trade Commission Act and GLBA were intended to protect and the type of harm that resulted from the Data Breach was the type of harm that the statutes were intended to guard against.

382. Defendants' violation of Section 5 of the FTC Act and GLBA constitutes negligence.

383. The FTC has pursued enforcement actions against businesses, which, as a result 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 the Class.

384. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

385. It was foreseeable that Defendants' 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 insurance industry.

386. Defendants have full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

387. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendants' systems or transmitted through third party systems.

388. 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.

389. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendants' possession.

390. Defendants were in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

391. Defendants' duty extended to protecting Plaintiffs and the Class 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.

392. Defendants have admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

393. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

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

395. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) uncompensated 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) some Plaintiffs' Private Information being disseminated on the dark web, according to Credit Karma and Experian; (viii) experiencing an increase in spam calls, texts, and/or emails; (ix) nominal damages; and (x) 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 Defendants' possession and is subject to further unauthorized disclosures so

long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

396. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff sand the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

397. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

398. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants 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
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class)

399. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein, and brings this claim solely against Liberty Bankers and Accendo ("Defendants" for the purposes of this count).

400. Plaintiffs and Class Members were required to deliver their Private Information to Defendants as part of the process of obtaining insurance products or services provided by Defendants. Plaintiffs and Class Members paid money to Defendants in exchange for products or services and would not have paid for Defendants' products or services, or would have paid less for them, had they known that Defendants' data security practices were substandard.

401. Defendants solicited, offered, and invited Class Members to provide their Private Information as part of Defendants' regular business practices. Plaintiffs and Class Members accepted Defendants' offers and provided their Private Information to Defendants as part of their express contracts for insurance services.

402. Defendants accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing services to Plaintiffs and Class Members.

403. Plaintiffs and the Class entrusted their Private Information to Defendants. In so doing, Plaintiffs and the Class entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Class if their data had been breached and compromised or stolen.

404. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations (including FTC guidelines and GLBA on data security) and were consistent with industry standards.

405. Implicit in the agreement between Plaintiffs and Class Members and Defendants to provide Private Information was Defendants' obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses, (f) retain the Private Information only under conditions that kept such information secure and confidential.

406. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendants, on the other, is demonstrated by their conduct and course of dealing.

407. On information and belief, at all relevant times Defendants promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

408. On information and belief, Defendants further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' Private Information would remain protected.

409. Plaintiffs and Class Members paid money to Defendant with the reasonable belief and expectation that Defendants would use part of their earnings to obtain adequate data security. Defendants failed to do so.

410. Plaintiffs and Class Members would not have entrusted their Private Information to Defendants in the absence of the implied contract between them and Defendants to keep their information reasonably secure.

411. Plaintiffs and Class Members would not have entrusted their Private Information to Defendants in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

412. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendants.

413. Defendants breached the implied contracts they made with Plaintiffs and the Class by failing to safeguard and protect their personal information, by failing to delete the information

of Plaintiffs and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

414. Every contract has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

415. Defendants breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard Private Information, failing to timely and accurately disclose the Data Breach to Plaintiffs and Class Members and continued acceptance of Private Information and storage of other personal information after Defendants knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

416. As a direct and proximate result of Defendants' breach of the implied contracts, Plaintiffs and Class Members sustained damages, including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) uncompensated 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) some Plaintiffs' Private Information being disseminated on the dark web; (viii) experiencing an increase in spam calls, texts, and/or emails; (ix) nominal damages; and (x) 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 Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

417. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

418. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class)

419. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein, and brings this claim against all Defendants.

420. Plaintiffs bring this claim in the alternative to the breach of implied contract claim above.

421. Plaintiffs and Class Members conferred a monetary benefit on Defendants. Specifically, they paid Landmark's clients, including Liberty Bankers and Accendo, for products or services and, in so doing, also provided Defendants with their highly valuable Private Information. In exchange, Plaintiffs and Class Members should have received from Landmark, Liberty Bankers, and Accendo the products or services that were the subject of the transaction, as well as adequate data security necessary to safeguard their Private Information.

422. Defendants knew that Plaintiffs and Class Members conferred a benefit upon them and accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendants profited from Plaintiffs' retained data and used Plaintiffs' and Class Members' Private Information for business purposes.

423. Defendants failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their Private Information provided.

424. Defendants acquired the Private Information through inequitable record retention as they failed to investigate and/or disclose the inadequate data security practices previously alleged.

425. If Plaintiffs and Class Members had known that Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would have entrusted their Private Information at Defendants or obtained products or services at Landmark's clients, including Liberty Bankers and Accendo.

426. Plaintiffs and Class Members have no adequate remedy at law.

427. Defendants enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendants instead calculated to increase their own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to their own profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize their own profits over the requisite security and the safety of their Private Information.

428. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon them.

429. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy;

(ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) uncompensated 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) some Plaintiffs' Private Information being disseminated on the dark web; (viii) experiencing an increase in spam calls, texts, and/or emails; (ix) nominal damages; and (x) 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 Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information.

430. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendants from their wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

431. Plaintiffs and Class Members may not have an adequate remedy at law against Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT IV
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On behalf of Plaintiffs and the Nationwide Class)

432. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein, and brings this claim against solely against Landmark.

433. Landmark entered into various contracts with its insurance carrier clients to provide administrative services. As a material part of those contracts, Landmark agreed to implement reasonable data security practices and procedures sufficient to safeguard the Private Information provided to it by its clients.

434. These contracts are virtually identical to each other and the provisions regarding Private Information were made expressly for the benefit of Plaintiffs and the Class, as it was their confidential information that Landmark agreed to collect and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class were the direct and primary objective of the contracting parties.

435. Landmark knew that if it were to breach these contracts, its clients' consumers, including Plaintiffs and the Class, would be harmed by, among other things, fraudulent misuse of their Private Information.

436. Landmark breached its contracts with its clients when it failed to use reasonable data security measures that could have prevented the Data Breach and resulting compromise of Plaintiffs' and Class Members' Private Information.

437. As a reasonably foreseeable result of the breach, Plaintiffs and the Class were harmed by Landmark's failure to use reasonable data security measures to store their Private Information, including but not limited to, the actual harm sustained from the loss of their Private Information to cybercriminals.

438. Accordingly, Plaintiffs and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

COUNT V
BREACH OF CONFIDENCE
(On Behalf of Plaintiffs and the Nationwide Class)

439. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein, and brings this claim against all Defendants.

440. As alleged herein and above, Defendants' relationship with Plaintiffs and the Class was governed by terms and expectations that Plaintiffs' and the Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

441. Plaintiffs and the Class entrusted Defendants with their Private Information with the explicit and implicit understandings that Defendants would protect and not permit the Private Information to be disseminated to any unauthorized third parties.

442. Plaintiffs and the Class also entrusted Defendants with their Private Information with the explicit and implicit understandings that Defendants would take precautions to protect that Private Information from unauthorized disclosure.

443. Defendants voluntarily received Plaintiffs' and Class Members' Private Information in confidence with the understanding that their Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

444. As a result of Defendants' failure to prevent and avoid the Data Breach from occurring, Plaintiffs' and Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

445. As a direct and proximate cause of Defendants' actions and/or omissions, Plaintiffs and the Class have suffered damages.

446. But for Defendants' disclosure of Plaintiffs' and Class Members' Private Information in violation of the parties' understanding of confidence, their Private Information

would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendants' Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' Private Information as well as the resulting damages.

447. The injury and harm Plaintiffs and the Class suffered was the reasonably foreseeable result of Defendants' unauthorized disclosure of Plaintiffs' and Class Members' Private Information. Defendants knew or should have known their methods of accepting and securing Plaintiffs' and Class Members' Private Information was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiffs' and Class Members' Private Information.

448. As a direct and proximate result of Defendants' breach of confidence with Plaintiffs and the Class, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information of current and former people; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information

compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

449. As a direct and proximate result of Defendants' breaches of confidence, Plaintiffs and the 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.

COUNT VI
INTRUSION UPON SECLUSION/INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Nationwide Class)

450. Plaintiffs re-allege and incorporate by reference all preceding allegations, as if fully set forth herein, and brings this claim against all Defendants.

451. Plaintiffs and Class Members had a reasonable expectation of privacy in their Private Information Defendant mishandled.

452. Defendant's conduct as alleged above intruded upon Plaintiffs' and Class Members' seclusion under common law.

453. By intentionally failing to keep Plaintiffs' and Class Members' Private Information safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiffs' and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiffs' and Class Members' private affairs in a manner that identifies Plaintiffs and Class Members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiffs and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiffs and Class Members.

454. Defendant knew that an ordinary person in Plaintiffs' or Class Members' position would consider Defendant's intentional actions highly offensive and objectionable.

455. Defendant invaded Plaintiffs' and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' private affairs by intentionally misusing and/or disclosing their Private Information without their informed, voluntary, affirmative, and clear consent.

456. Defendant intentionally concealed from, and delayed reporting to, Plaintiffs and Class Members a security incident that resulted in the unauthorized disclosure and misuse of their Private Information without their informed, voluntary, affirmative, and clear consent.

457. The conduct described above was at or directed at Plaintiffs and the Class Members.

458. As a proximate result of such intentional misuse and disclosures, Plaintiffs' and Class Members' reasonable expectations of privacy in their Private Information was unduly frustrated and thwarted. Defendant's conduct amounted to a substantial and serious invasion of Plaintiffs' and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendant's intentional actions or inaction highly offensive and objectionable.

459. In failing to protect Plaintiffs' and Class Members' Private Information, and in intentionally misusing and/or disclosing their Private Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private. Plaintiffs, therefore, seek an award of damages on behalf of themselves and the Nationwide Class.

460. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendants and that the Court grants the following:

A. For an Order certifying the Class, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members;

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

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

ii. requiring Defendants 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 Defendants to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendants to provide out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information for Plaintiffs' and Class

Members' respective lifetimes;

v. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;

vi. prohibiting Defendants from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;

vii. requiring Defendants 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 Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

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

ix. requiring Defendants to audit, test, and train their security personnel regarding any new or modified procedures;

x. requiring Defendants to segment data by, among other things, creating firewalls and controls so that if one area of Defendants' network is compromised, hackers cannot gain access to portions of Defendants' systems;

xi. requiring Defendants to conduct regular database scanning and securing checks;

xii. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees'

respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xiii. requiring Defendants to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiv. requiring Defendants to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

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

xvi. requiring Defendants to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvii. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and

xviii. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' 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. For an award of damages, including actual, nominal, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

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

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all claims so triable.

Dated: May 13, 2025

Respectfully Submitted,

/s/ Joe Kendall

JOE KENDALL
Texas Bar No. 11260700
KENDALL LAW GROUP, PLLC
3811Turtle Creek Blvd., Suite 825
Dallas, Texas 75219
214-744-3000 / 214-744-3015 (Facsimile)
jkendall@kendalllawgroup.com

Tyler J. Bean*
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, NY 10151
T: 929-677-5144
tbean@sirillp.com

A. Brooke Murphy*
MURPHY LAW FIRM
4116 Will Rogers Pkwy, Suite 700
Oklahoma City, OK 73108

Telephone: (405) 389-4989
abm@murphylegalfirm.com

Gary Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
gklinger@milberg.com

Attorneys for Plaintiffs and the Proposed Class

**Pro hac vice applications forthcoming*