

Exhibit A

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION**

CARY WEIGAND, CHERYL SCHMIDT)	JURY TRIAL DEMANDED
and CALVIN SCHMIDT, individually,)	
and on behalf of a class of similarly)	
situated persons,)	
)	
<i>Plaintiffs,</i>)	
v.)	Civil Action No. _____
)	
GROUP 1001 INSURANCE HOLDINGS,)	
LLC;)	
GROUP 1001 RESOURCES, LLC;)	
CLEAR SPRING LIFE AND ANNUITY)	
COMPANY;)	
-and-)	
DELAWARE LIFE INSURANCE)	
COMPANY)	
)	
<i>Defendants.</i>)	

CLASS ACTION COMPLAINT

Plaintiffs, CAREY WEIGAND (“Plaintiff Weigand”), CHERYL SCHMIDT (“Plaintiff Cheryl Schmidt”), and CALVIN SCHMIDT (“Plaintiff Calvin Schmidt”) (collectively, “Plaintiffs”), individually and on behalf of all others similarly situated, bring this class action against Defendants, GROUP 1001 INSURANCE HOLDINGS, LLC, GROUP 1001 RESOURCES, LLC (collectively “Group 1001”), CLEAR SPRING LIFE AND ANNUITY COMPANY (“Clear Spring”), and DELAWARE LIFE INSURANCE COMPANY (“Delaware Life”) (collectively, “Defendants”) and their present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, members, and/or other related entities, and upon personal knowledge as to their own actions, and information and belief as to all other matters, allege as follows:

INTRODUCTION

1. This action arises out of the public exposure of the confidential, personal information of Defendants' current, former and prospective customers and employees, and employee dependents, Personally Identifying Information¹ ("PII") (hereinafter, "Private Information"), including Plaintiffs and the proposed Class Members, on or about February 9, 2023, and as early as November 30, 2022, during a ransomware cyberattack to Defendants' systems, caused by Defendants' collective failures to adequately safeguard that information ("the Data Breach").²

2. According to Defendants, the Private Information unauthorizedly disclosed in the Data Breach includes customers' and/or employees' (and their dependents') names, addresses, dates of birth, Social Security numbers, and contract/policy numbers³ as well as their financial account numbers or credit/debit card numbers (in combination with security code, access code,

¹ The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8). To be clear, according to Defendants, not every type of information included in that definition was compromised in the Data Breach.

² See: "Group 1001 Resumes Full Operations After Ransomware Attack," March 1, 2023, available at <https://www.group1001.com/news/group-1001-resumes-full-operations-after-ransomware-attack> (last accessed August 15, 2023), **attached as Exhibit A**;

Clear Spring Life and Annuity Company, "Notice of Data Breach," Cary Weigand, July 28, 2023, **attached as Exhibit B**;

Clear Spring Life and Annuity Company, "Notice of Data Breach," Cheryl Schmidt, July 28, 2023, **attached as Exhibit C**;

Delaware Life Insurance Company, "Notice of Data Breach," Calvin Schmidt, July 28, 2023, **attached as Exhibit D**;

Group 1001 Resources LLC, sample Notice of Data Breach, July 28, 2023, available at <https://apps.web.maine.gov/online/aeviewer/ME/40/fce1bd8e-b164-458e-bb3d-42b5dcaeb0a4.shtml> **attached as Exhibit E**.

³ See: "Notice of Data Breach," Ex. B; "Notice of Data Breach," Ex. C; "Notice of Data Breach," Ex. D.

password or pin for the account)⁴, and their Driver's License Numbers or Non-Driver Identification Card Numbers, passport number, insurance, and other benefits information, such as the names of dependents and beneficiaries.⁵

3. Based in Zionsville, Indiana, Group 1001 “is an insurance holding company [which] through its subsidiaries, provides an array of protection and wealth accumulation products, such as annuities, life insurance, and property and casualty insurance.”⁶

4. Group 1001’s subsidiaries and “insurance brands” include Defendants Clear Spring Life and Annuity Company (“Clear Spring”), and Defendants Delaware Life Insurance Company (“Delaware Life”), through whom Defendants provide life and annuity insurance products to customers.⁷

5. As a condition of purchasing an annuity contract or life insurance policy from Group 1001, Clear Spring, and/or Delaware Life, Defendants required their customers and prospective customers to provide them with their sensitive Private Information, which Defendants promised to protect from unauthorized disclosure.

6. In addition, as a condition of employment, Defendants required prospective employees and employees to provide them with their Private Information, which Defendants promised to protect from unauthorized disclosure.

7. Defendants failed to undertake adequate measures to safeguard the Private

⁴ See Clear Spring Notice to Maine Attorney General, July 27, 2023, avail. at <https://apps.web.maine.gov/online/aewiewer/ME/40/5f16f55f-42b7-458f-a916-2603c9f83bb7.shtml> (last acc. Aug. 15, 2023)

⁵ See Group 1001 Data Breach Notification to Maine Attorney General, July 28, 2023, avail. at <https://apps.web.maine.gov/online/aewiewer/ME/40/fce1bd8e-b164-458e-bb3d-42b5dcaeb0a4.shtml> (last acc. Aug. 15, 2023).

⁶ Group 1001 Privacy Policy, avail. at <https://www.group1001.com/legal/> (last acc. Aug. 15, 2023).

⁷ See <https://www.group1001.com/careers> (last acc. Aug. 15, 2023).

Information of Plaintiffs and the proposed Class Members, including failing to implement industry standards for data security, and failing to properly train employees on cybersecurity protocols, resulting in the Data Breach.

8. Although Defendants purportedly discovered the Data Breach on February 9, 2023, they uniformly failed to immediately notify and warn current, former, and prospective customers and employees who were victimized in the breach, waiting until July 28, 2023 to send written notice to Plaintiffs and the Class Members.⁸

9. As a direct and proximate result of Defendants' failures to protect current, prospective, and former customers' and employees' sensitive Private Information and warn them promptly and fully about the Data Breach, Plaintiffs and the proposed Class Members have suffered widespread injury and damages necessitating Plaintiffs to seek relief on a class wide basis.

PARTIES

10. Plaintiff Weigand is a natural person and resident and citizen of the State of Oregon, residing in Bandon, Coos County, Oregon, where she intends to remain. Plaintiff is a customer of Clear Spring and Group 1001 and a Data Breach victim.

11. Plaintiff Cheryl Schmidt is a natural person and resident and citizen of the State of Minnesota, residing in Cold Spring, Stearns County, Minnesota, where she intends to remain. Plaintiff is a customer of Clear Spring, Delaware Life, and Group 1001 and a Data Breach victim.

12. Plaintiff Calvin Schmidt is a natural person and resident and citizen of the State of Minnesota, residing in Cold Spring, Stearns County, Minnesota, where he intends to remain. Plaintiff is a customer of Delaware Life, Clear spring, and Group 1001 and a Data Breach victim.

⁸ See: "Notice of Data Breach," Ex. B; "Notice of Data Breach," Ex. C; "Notice of Data Breach," Ex. D.

13. Defendant Group 1001 Insurance Holdings, LLC, is a limited liability company organized and existing under the laws of the State of Delaware with a principal place of business at 10555 Group 1001 Way, Zionsville, Indiana, 46077.

14. On information and belief, Defendant Group 1001 Resources, LLC, is a limited liability company organized and existing under the laws of the State of Delaware with a principal place of business at 10555 Group 1001 Way, Zionsville, Indiana, 46077, which manages Group 1001 Insurance Holdings, LLC's workforce (Defendants Group 1001 Insurance Holdings, LLC and Group 1001 Resources, LLC are collectively referred to as "Group 1001").

15. On information and belief, Clear Spring is a corporation organized and existing under the laws of the State of Delaware with a principal place of business at 10555 Group 1001 Way, Zionsville, Indiana 46077.

16. Delaware Life is a corporation organized and existing under the laws of the State of Delaware with a principal place of business at 1601 Trapelo Road, Suite 30, Waltham, Massachusetts 02451, and, upon information and belief, with an office located at 10555 Group 1001 Way, Zionsville, Indiana 46077.

17. As follows, Clear Spring and Delaware Life are subsidiary companies of Group 1001. On information and belief, Defendants are all *alter egos* of one another.

JURISDICTION & VENUE

18. This Court has personal jurisdiction over Defendants Group 1001 and Clear Spring because each operates, conducts, engages in, or carries on a business in Indiana, and each maintains a principal place of business in this State.

19. This Court has personal jurisdiction over Defendant Delaware Life because it operates, conducts, engages in, or carries on a business in this State; caused personal injury or

property damage by an act or omission done within this state or caused personal injury or caused personal injury or property damage in this state by an occurrence, act or omission done outside this state while regularly doing business in this state; by having supplied or contracted to supply services rendered in this state; and by owning, using, or possessing any real property within this state.

20. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of \$5,000,000, exclusive of interest and costs, there are more than one hundred (100) members in the proposed Class, and at least one member of the class is a citizen of a state different from Defendants.

21. The Court has supplemental jurisdiction over Plaintiff's claims arising under state law under 28 U.S.C. § 1367.

22. Venue is proper under 28 U.S.C. § 1391(b) because Defendants Group 1001 and Clear Spring reside in this district and a substantial part of the events and omissions giving rise to Plaintiffs' claims occurred in this district.

BACKGROUND FACTS

A. Defendants, Group 1001, Clear Spring, and Delaware Life

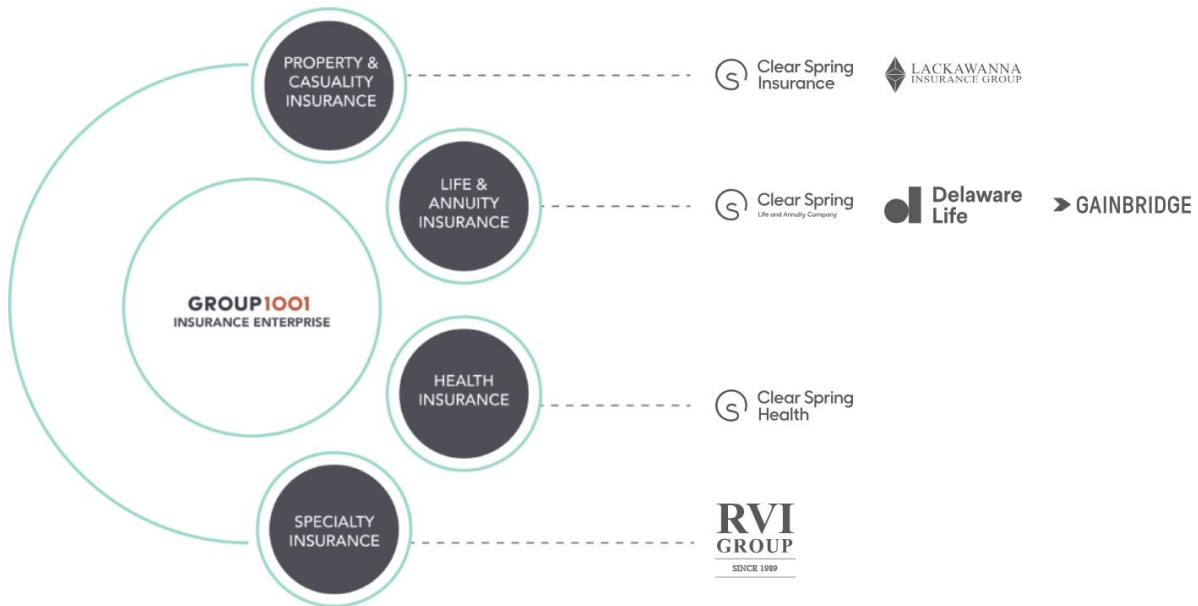
23. Group 1001 holds itself out as a “technology-driven financial services company with a mission to empower our customers, employees, and communities by making innovative products accessible to everyone [; and] striv[ing] to demystify how insurance and annuity products are purchased today by leveraging technology to provide intuitive financial solutions for all Americans.”⁹

24. Group 1001 provides financial products and services to customers such as

⁹ <https://www.group1001.com/> (last acc. Aug. 15, 2023)

annuities, life insurance, and property and casualty insurance through its subsidiary companies, including Clear Spring and Delaware Life.¹⁰

25. As Group 1001 explains, the relationship between it and its subsidiary companies, Clear Spring and Delaware Life, is as follows:



11

26. Indeed, Clear Spring states that it is “a Delaware-domiciled life insurance company that is a subsidiary of Group 1001 Insurance Holdings, LLC, which, along with its affiliates, does business under the name, Group 1001.”¹²

27. Clear Spring offers a financial products, namely annuities such as ClearFlex Fixed Indexed Annuity, ViStar Fixed Indexed Annuity, Highlander Fixed Indexed Annuity, Highlander 7 Fixed Indexed Annuity, Preserve Multi-Year Generational Annuity, and the Provider Single Premium Immediate Annuity.¹³

¹⁰ <https://www.group1001.com/#companies>; <https://www.group1001.com/careers/>

¹¹ <https://www.group1001.com/careers>

¹² Clear Spring, “Terms and Conditions,” avail. at <https://clearspringlife.com/terms-conditions>

¹³ <https://clearspringlife.com/products>

28. Likewise, according to Delaware Life, “[f]ounded in 2013, [it] is a member of Group One Thousand One, LLC (“Group1001”): A dynamic network of businesses making insurance more useful, logical and accessible for everyone.”¹⁴

29. Delaware Life specializes in “retirement services and helping people achieve their long-term financial goals,”¹⁵ offering annuity products including fixed asset annuities (Growth Pathway Fixed Index Annuity, Retirement Stages Select, Target Income 10, and Target Growth 10), as well as Multi-year Guaranteed Fixed Annuities, and Variable Annuities.¹⁶

30. As of December 2022, Delaware Life managed total assets of \$41.2 billion with over 334,000 annuity and life insurance policies.¹⁷

31. As a condition of receiving Defendants’ annuity services, Group 1001, Clear Spring, and Delaware Life each require that their customers and employees provide Defendants with their Private Information, including their names, addresses, dates of birth, Social Security numbers, and contract/policy numbers, as well as their financial account numbers or credit/debit card numbers, and their Driver's License Numbers or Non-Driver Identification Card Numbers, passport number, insurance, and other benefits information, such as the names of dependents and beneficiaries.

32. Defendants collect and store this Private Information on their information technology computer systems, on information and belief located at 10555 Group 1001 Way, Zionsville, Indiana 46077.

33. Defendants promise customers and prospective customers and employees that they will take adequate measures to safeguard their Private Information.

¹⁴ <https://www.delawarelife.com/home> (last acc. Aug. 15, 2023).

¹⁵ <https://www.delawarelife.com/content/our-story> (last acc. Aug. 15, 2023).

¹⁶ <https://www.delawarelife.com/our-products/all-annuities-page> (last acc. Aug. 15, 2023).

¹⁷ <https://www.delawarelife.com/home> (last acc. Aug. 15, 2023).

34. On information and belief, Group 1001 maintains policies concerning the privacy of the Private Information it collects from customers and prospective customers, including that it will use this information only for certain purposes, none of which include the Data Breach, and in which it represents having technical safeguards designed to protect their Private Information.

35. Clear Spring maintains a Privacy Policy (“Clear Spring Privacy Policy”), which applies “...to information we collect via Clear Spring Life websites or online services that display or link to this Notice (the “Services”). This Notice also applies to communications you may have with us.”¹⁸

36. In its Privacy Policy, Clear Spring informs customers and prospective customers that:

We collect personal information from you when you use our Services and interact with us. The information we collect includes: any information you choose to provide us, such as first and last name, account name, address, Social Security number, contact information (e.g., telephone number) and any interest you may express in our products and services. In some circumstances, we may be required to collect information such as government-issued ID and proof of address. We may also collect information relating to:

- Records and copies of your correspondence (including email addresses and audio recordings of calls placed to our customer service representatives), if you contact us.
- Your responses to surveys, such as those that we might ask you to complete for research purposes.
- Details of potential transactions or transactions you carry out through us or financial products and services you purchase, including financial information.¹⁹

37. Clear Spring’s Privacy Policy provides enumerated purposes for which it may use customers’ Private Information, including providing services to customers, responding to inquiries, and for business purposes including authenticating identities and access to accounts;

¹⁸ Clear Spring Privacy Policy, Effective January 1, 2021, available at <https://clearspringlife.com/privacy-policy> (last acc. Aug. 15, 2023), **attached as Exhibit F.**

¹⁹ *Id.*

“Initiating, facilitating, processing, and/or executing transactions; Responding to your requests and questions; Communicating with you regarding your account or any Services you use; Performing creditworthiness, fraud prevention or other similar reviews; Evaluating applications; Comparing information for accuracy and verification purposes; Managing our business and protecting ourselves, you, other persons, and the Services; Providing a personalized experience and implementing your preferences; Better understanding our customers and how they use and interact with the Services; Complying with our policies and obligations, government orders, legal advice or legal process; Establishing, exercising or defending our legal rights where it is necessary for our legitimate interests or the legitimate interests of others; Resolving disputes, collecting fees, or troubleshooting problems; and Providing customer service to you or otherwise communicating with you[;] and to “fulfill the purposes for which you provide it, or with your consent.”²⁰

38. None of the purposes for which Clear Spring is permitted to use customer’s Private Information under its Privacy Policy include the Data Breach.

39. Further, in its Privacy Policy, Clear Spring explicitly states that it has “implemented administrative, physical and technical safeguards designed to protect your personal information.”²¹

40. Delaware Life maintains a Privacy Policy (“Delaware Life Privacy Policy”), in which it states:

At Delaware Life, protecting your privacy is important to us. Whether you are an existing customer or considering a relationship with us, we recognize that you have an interest in how we may collect, use and share information about you. **We understand and appreciate the trust and confidence you place in us, and we take seriously our obligation to maintain the confidentiality and security of your personal information.** We invite you to review this Privacy Policy which outlines how we use and protect that information.²²

²⁰ *Id.*

²¹ *Id.*

²² Delaware Life Privacy Policy, avail. at <https://www.delawarelife.com/static/documents/DLIC-Privacy-Policy.pdf> (last acc. Aug. 15, 2023) (emphasis added), **attached as Exhibit G.**

41. In its Privacy Policy, Delaware Life represents to customers and prospective customers that:

Collecting personal information from you is essential to our ability to offer you high-quality investment, retirement and insurance products. When you apply for a product or service from us, we need to obtain information from you to determine whether we can provide it to you. As part of that process, we may collect information about you, known as nonpublic personal information, from the following sources:

- Information we receive from you on applications or other forms, such as your name, address, social security number and date of birth;
- Information about your transactions with us, our affiliates or others, such as other life insurance policies or annuities that you may own; and
- Information we receive from a consumer reporting agency, such as a credit report.²³

42. Delaware Life’s Privacy Policy states that “[o]nce we obtain nonpublic personal information from you, we do not disclose it to any third party except as permitted or required by law...[;]” and provides certain enumerated purposes for which it may share this Private Information with third parties, including “to companies that help in conducting our business or perform services on our behalf” in which case it “require[s] them to comply with strict standards regarding the security and confidentiality of our customers’ nonpublic personal information[;] when complying with federal, state or local laws, when responding to a subpoena, or when complying with an inquiry by a governmental agency or regulator.”²⁴

43. In its Privacy Policy, Delaware Life goes on to represent and promise customers that, “[w]e maintain physical, electronic and procedural safeguards that comply with federal and state regulations to safeguard your nonpublic personal information from unauthorized use or improper access.”²⁵

44. Moreover, Delaware Life’s Privacy Policy states that it will not disclose nonpublic

²³ *Id.*

²⁴ *Id.*

²⁵ *Id.*

Private Information to non-affiliated third parties even after the customer relationship ends.²⁶

45. None of the purposes for which Delaware Life is permitted to disclose customer's Private Information under its Privacy Policy includes the Data Breach.

46. Despite their representations to employ adequate safeguards to protect customers' Private Information, including as set forth in their privacy policies and, Defendants do not follow industry standard practices in securing that information stored in their information technology systems.

B. Defendants Fail to Safeguard Customers' and Employees' Private Information

47. On or about February 9, 2023, and possibly as early as November 30, 2022, unauthorized third party cybercriminals were able to access the systems of Defendants, Group 1001, Clear Spring, and Delaware Life, during a ransomware cyberattack and acquire the Private Information of current, former, and prospective customers, and employees (and dependents), including their names, addresses, dates of birth, Social Security numbers, contract/policy numbers, as well as their financial account numbers or credit/debit card numbers (in combination with security code, access code, password or pin for the account), and their Driver's License Numbers or Non-Driver Identification Card Numbers ("the Data Breach").²⁷

48. The Data Breach was the result of Defendants' collective failures to safeguard the Private Information of its current, former, and prospective customers and employees, including by failing to utilize industry standard data security measures, and failing to properly train employees

²⁶ *Id.*

²⁷ See Clear Spring Notice of Data Breach, Cary Weigand, Exhibit B; Clear Spring Notice of Data Breach, Cheryl Schmidt, Exhibit C; Delaware Life Notice of Data Breach, Calvin Schmidt, Exhibit D; Clear Spring Data Breach Notification to Maine Attorney General, July 27, 2023, available at <https://apps.web.maine.gov/online/aewiewer/ME/40/5f16f55f-42b7-458f-a916-2603c9f83bb7.shtml> (last acc. Aug. 15, 2023); Group 1001, sample Notice of Data Breach, July 28, 2023, avail. at <https://apps.web.maine.gov/online/aewiewer/ME/40/fce1bd8e-b164-458e-bb3d-42b5dcaeb0a4.shtml>.

on cybersecurity protocols.

i. Group 1001 Website Notice of the Data Breach

49. On March 1, 2023, Group 1001 posted a notice on its website (“Website Notice”), stating that it was providing an update as to the Data Breach experienced by Defendants, *to wit*, “concerning recent system interruptions experienced by certain Group 1001 Insurance member companies, including Delaware Life Insurance Company, Delaware Life Insurance Company of New York, Clear Spring Life and Annuity Company, Clear Spring Property and Casualty Company, and our Clear Spring Health business.”²⁸

50. The Website Notice stated that “[b]eginning on February 9, 2023, we were alerted to the existence of sophisticated ransomware on our information technology infrastructure,” after which it “immediately launched an investigation to determine the full scope of the incident, and a team of third-party forensic experts was engaged to assist in the investigation...”²⁹

51. Group 1001’s Website Notice went onto state that after discovering the Data Breach, it:

- We took immediate action by proactively disconnecting systems from our network to contain the threat and prevent additional systems from being affected.
- Along with our forensics experts, our team scanned systems for indicators of compromise and remediated any identified indicators of compromise.
- In addition, we deployed additional advanced endpoint detection and monitoring tools on our newly restored systems for an added layer of security and visibility across our network.
- All systems were validated as clean by conducting additional scans

²⁸ “Group 1001 Resumes Full Operations After Ransomware Attack,” March 1, 2023, available at <https://www.group1001.com/news/group-1001-resumes-full-operations-after-ransomware-attack> (last accessed August 15, 2023), **Exhibit A**.

²⁹ *Id.*

before they were brought back online.

- We have been, and continue to be, in communication with our regulators about this incident.
- There will be a number of other infrastructure enhancements to continuously strengthen the security posture of Group 1001's network and systems in the days, months, and years ahead.³⁰

52. The Website Notice too informed stakeholders that it has notified the Federal Bureau of Investigation of the Data Breach, that it did not pay a ransom, and stating that, “[t]he security of our information and that of our contract holders and other stakeholders is important to us. Once our investigation is complete, we will notify any impacted parties as appropriate.”³¹

53. On or about July 27, 2023, Clear Spring reported the Data Breach to the Maine Attorney General, reporting that the Data Breach occurred on February 9, 2023, and was discovered that day; that it occurred by an “external system breach (hacking)” and ransomware attack; that 4,393 persons were affected; and that the information acquired included “Name or other personal identifier in combination with: Financial Account Number or Credit/Debit Card Number (in combination with security code, access code, password or PIN for the account).”³²

54. On or about July 28, 2023, Group 1001, as “Group 1001 Resources, Inc.” or “Group 1001 Resources, LLC,” reported the Data Breach to the Maine Attorney General, reporting that the Data Breach occurred beginning on November 30, 2022; was discovered on February 9, 2023; involved an external system breach (hacking) attack; and that the information acquired included *employees*' and dependents' “Name[s] or other personal identifier in combination with: Driver's

³⁰ *Id.*

³¹ *Id.*

³² Clear Spring Data Breach Notification to Maine Attorney General, July 27, 2023, available at <https://apps.web.maine.gov/online/aewviewer/ME/40/5f16f55f-42b7-458f-a916-2603c9f83bb7.shtml>

License Number[s] or Non-Driver Identification Card Number[s]”³³ and/or passport number, insurance, and other benefits information, such as the names of your dependents and beneficiaries.³⁴

55. On information and belief, the Data Breach that was reported as occurring on February 9, 2023 involving Clear Spring and the Data Breach to Group 1001’s systems from November 30, 2022 to February 9, 2023 was the same event impacting the Private Information of Defendants’ prospective, current, and former customers and employees.

56. Despite discovering the Data Breach on February 9, 2023, Clear Spring and Delaware Life waited until July 28, 2023, to begin sending written notification to prospective, current and former customers impacted by the Data Breach.

57. Likewise, despite discovering the Data Breach on February 9, 2023, Group 1001 waited until July 28, 2023, to begin sending written notification to prospective, current and former employees impacted by the Data Breach.

ii. Clear Spring’s Data Breach Notice

58. On or about July 28, 2023, Clear Spring began sending written notification of the Data Breach to affected current, former, and prospective customers associated with an annuity or life insurance contract, stating that:

On February 9, 2023, we were alerted to the existence of sophisticated ransomware on our information technology infrastructure. We immediately took steps to isolate and secure our systems and investigate the incident. We retained a leading third-party forensics firm to conduct a thorough investigation, secure our systems, remediate any risks, and methodically bring our systems back online once such systems were validated as clean. We also alerted appropriate regulatory authorities and the Federal Bureau of investigation.³⁵

³³ Group 1001 Data Breach Notification to Maine Attorney General, July 28, 2023, available at <https://apps.web.maine.gov/online/aeviewer/ME/40/fce1bd8e-b164-458e-bb3d-42b5dcaeb0a4.shtml> (emphasis added).

³⁴ *Id.*, sample Data Breach Notice, July 28, 2023.

³⁵ Clear Spring Data Breach Notice to Cheryl Schmidt, Ex. B; Clear Spring Data Breach Notice

59. Clear Spring's Data Breach Notice went onto explain that its investigation determined that in the Data Breach discovered on February 9, 2023, "an unauthorized malicious actor accessed and acquired certain files from our systems," which after further investigation completed on July 10, 2023 was determined to involve Private Information which "differ[ed] from individual to individual but may have included" their names, addresses, dates of birth, Social Security numbers, and contract/policy numbers."³⁶

60. In its Data Breach Notice, Clear Spring further stated that they had "scanned our systems for, and remediated, any identified indicators of compromise[;]" and "deployed additional advanced endpoint detection and monitoring tools on our newly restored systems for an added layer of security and visibility across our network[;]" and would continue to make infrastructure enhancements.³⁷

61. Clear Spring's Data Breach Notice went on to state it had not "identified any suspicious activity pertaining to your associated annuity contract or life insurance policy and [had] not received any reports of misuse of your information," but nevertheless encouraged Data Breach victims to be "vigilant and closely review and monitor [] financial accounts, statements, credit reports, and other financial information for any evidence of unusual activity, fraudulent charges, or signs of identity theft."³⁸

62. Clear Spring's Data Breach Notice likewise apprised Data Breach Victims of their abilities to put a fraud alert or security freeze on their credit files.³⁹

to Cary Weigand, Ex. C.

³⁶ *Id.*

³⁷ *Id.*

³⁸ *Id.*

³⁹ *Id.*

63. Further, in the Data Breach Notice, Clear Spring offered affected victims two (2) years of identity theft protection services through IDX.⁴⁰

64. Clear Spring's Data Breach Notice was signed by Robert Stanton, labeled as the Chief Operating Officer of Clear Spring. In reality,

iii. Delaware Life's Data Breach Notice

65. As with Clear Spring, on or about July 28, 2023, Delaware Life began sending written notification of the Data Breach to affected current, former, and prospective customers associated with an annuity or life insurance contract, which contained almost identical content as the Clear Spring Data Breach Notice.⁴¹

66. Indeed, Delaware Life stated, verbatim to Clear Spring's Data Breach Notice, stated:

On February 9, 2023, we were alerted to the existence of sophisticated ransomware on our information technology infrastructure. We immediately took steps to isolate and secure our systems and investigate the incident. We retained a leading third-party forensics firm to conduct a thorough investigation, secure our systems, remediate any risks, and methodically bring our systems back online once such systems were validated as clean. We also alerted appropriate regulatory authorities and the Federal Bureau of Investigation.⁴²

67. Likewise, Delaware Life's Data Breach Notice went onto explain that "an unauthorized malicious actor [had] accessed and acquired certain files from our systems," which after further investigation completed on July 10, 2023 was determined to involve Private Information which "differ[ed] from individual to individual but may have included" their names, addresses, dates of birth, Social Security numbers, and contract/policy numbers."⁴³

⁴⁰ *Id.*

⁴¹ *See* Delaware Life Insurance Company, "Notice of Data Breach," Calvin Schmidt, July 28, 2023, Exhibit D;

⁴² *Id.*

⁴³ *Id.*

68. In its Data Breach Notice, Delaware Life further stated that they had “scanned our systems for, and remediated, any identified indicators of compromise[;]” and “deployed additional advanced endpoint detection and monitoring tools on our newly restored systems for an added layer of security and visibility across our network[;]” and would continue to make infrastructure enhancements.⁴⁴

69. Delaware Life’s Data Breach Notice went on to state it had not “identified any suspicious activity pertaining to your associated annuity contract or life insurance policy and [had] not received any reports of misuse of your information,” but nevertheless encouraged Defendants’ Data Breach victims to be “vigilant and closely review and monitor [] financial accounts, statements, credit reports, and other financial information for any evidence of unusual activity, fraudulent charges, or signs of identity theft.”⁴⁵

70. Delaware Life’s Data Breach Notice likewise apprised Data Breach Victims of their abilities to put a fraud alert or security freeze on their credit files.⁴⁶

71. Further, in the Data Breach Notice, Delaware Life offered affected victims two (2) years of identity theft protection services through IDX.⁴⁷

iv. Group 1001’s Data Breach Notice

72. Further, on or about July 28, 2023, Group 1001 (Group 1001 Resources, LLC) began sending written notification of the Data Breach to affected employees, former employees, job applicants, or spouses, dependents, or beneficiary of an employee or former employee.⁴⁸

⁴⁴ *Id.*

⁴⁵ *Id.*

⁴⁶ *Id.*

⁴⁷ *Id.*

⁴⁸ See Group 1001 Resources, LLC, sample Notice of Data Breach, July 28, 2023, available at <https://apps.web.maine.gov/online/aeviewer/ME/40/fce1bd8e-b164-458e-bb3d-42b5dcaeb0a4.shtml>, **attached as Exhibit E.**

73. In verbatim language to both Clear Spring’s and Delaware Life’s Data Breach Notices, Group 1001 explained in its Data Breach Notice that, “[o]n February 9, 2023, we were alerted to the existence of sophisticated ransomware on our information technology infrastructure...[etc.]”⁴⁹

74. As with the prior data breach notices, Group 1001’s Data Breach Notice went onto explain that “an unauthorized malicious actor [had] accessed and acquired certain files from our systems,” which after further investigation completed on July 10, 2023 was determined to involve Private Information, **but that**, the information “differ[ed] from individual to individual but may have included” their names, addresses, dates of birth, Social Security numbers, driver’s license or passport numbers, insurance, and other benefits information, such as the names of your dependents and beneficiaries.⁵⁰

75. In its Data Breach Notice, Group 1001 further stated that they had “scanned our systems for, and remediated, any identified indicators of compromise[;]” and “deployed additional advanced endpoint detection and monitoring tools on our newly restored systems for an added layer of security and visibility across our network[;]” and would continue to make infrastructure enhancements.⁵¹

76. Group 1001’s Data Breach Notice encouraged Defendants’ Data Breach victims to be “vigilant and closely review and monitor [] financial accounts, statements, credit reports, and other financial information for any evidence of unusual activity, fraudulent charges, or signs of identity theft.”⁵²

⁴⁹ *Id.*

⁵⁰ *Id.*

⁵¹ *Id.*

⁵² *Id.*

77. Group 1001's Data Breach Notice likewise apprised Data Breach victims of their abilities to put a fraud alert or security freeze on their credit files.⁵³

78. Further, and as with Defendants' other data breach notices, in Group 1001's Data Breach Notice, it offered affected victims two (2) years of identity theft protection services through IDX.⁵⁴

79. On or about July 28, 2023, Group 1001 posted an updated to its prior Website Notice, to state that:

Over the past several months, we have been analyzing the impacted files since fully recovering our systems to understand what personal information may be at risk. We have begun the process of notifying the individuals whose personal information is confirmed to have been included. **Impacted individuals will soon be receiving a letter that will explain how to enroll in the following services.**

[...]

To help prevent a similar occurrence in the future, we have implemented numerous additional measures designed to enhance the security of our network, systems, and data.⁵⁵

iv. Plaintiffs' and the proposed Class Members' Private Information was unauthorizedly disclosed to third-party cybercriminals in the Data Breach

80. Plaintiffs' and the proposed Class Members' Private Information was unauthorizedly disclosed to third-party cybercriminals in Defendants' Data Breach, including their names, addresses, dates of birth, Social Security numbers, contract/policy numbers, as well as their financial account numbers or credit/debit card numbers (in combination with security code, access code, password or pin for the account), and their Driver's License Numbers or Non-Driver Identification Card Numbers ("the Data Breach").⁵⁶

⁵³ *Id.*

⁵⁴ *Id.*

⁵⁵ Group 1001, "Group 1001 Update on Ransomware Attack," avail. at <https://www.group1001.com/news/group-1001-update-on-ransomware-attack> (last acc. Aug. 15, 2023) (emphases added).

⁵⁶ See Clear Spring Notice of Data Breach, Cary Weigand, Exhibit B; Clear Spring Notice of Data Breach, Cheryl Schmidt, Exhibit C; Delaware Life Notice of Data Breach, Calvin Schmidt,

81. Defendants' conduct, by acts of commission or omission, caused the Data Breach, including: Group 1001's, Clear Spring's and Delaware Life's collective failures to implement best practices and comply with industry standards concerning computer system security to adequately safeguard Private Information, allowing Private Information to be accessed and stolen, by failing to implement security measures that could have prevented, mitigated, or timely detected the Data Breach, by failing to adequately train their customers on cybersecurity policies, enforce those policies, or maintain reasonable security practices and systems; and by Group 1001 failing to supervise its subsidiary companies, Clear Spring and Delaware Life, resulting in the Data Breach.

82. On information and belief, as more fully articulated below, Plaintiffs' and the members of the proposed Class Members' Private Information, unauthorizedly disclosed to third-party cybercriminals in the Data Breach, has now or will imminently be posted to the Dark Web for public viewing and use, in the public domain, and utilized for criminal purposes and fraudulent misuse.

C. Plaintiffs' Experiences

i. Plaintiff Weigand

83. Plaintiff Weigand was a customer of Defendants, having purchased a 10-year annuity from Clear Spring through Elevation Capital in November 2020.

84. As a condition of receiving Clear Spring's and Group 1001's financial services, Plaintiff Weigand was required to provide said Defendants with her Private Information, including but not limited to her name, address, date of birth, Social Security number, and contract/policy

Exhibit D; Clear Spring Data Breach Notification to Maine Attorney General, July 27, 2023, available at <https://apps.web.maine.gov/online/aewiewer/ME/40/5f16f55f-42b7-458f-a916-2603c9f83bb7.shtml> (last acc. Aug. 15, 2023); Group 1001 Notification to Maine Attorney General, July 28, 2023, avail. at <https://apps.web.maine.gov/online/aewiewer/ME/40/fce1bd8e-b164-458e-bb3d-42b5dcaeb0a4.shtml> (last acc. Aug. 15, 2023).

number.

85. In entrusting her Private Information to Clear Spring and Group 1001, Plaintiff Weigand believed that they would adequately safeguard that information, including as set forth in their privacy policies. Had Plaintiff Weigand known that Clear Spring and Group 1001 did not utilize reasonable data security measures, she would not have entrusted her Private Information to said Defendants.

86. Plaintiff Weigand received Clear Spring's Data Breach Notice dated July 28, 2023 (Ex. B) on August 2, 2023, informing her that her Private Information, including her name, address, date of birth, Social Security number, and contract/policy number were unauthorizedly disclosed to and acquired by cybercriminals in Defendants' Data Breach. *See Exhibit B.*

87. Plaintiff Weigand enrolled in the identity monitoring services with IDX offered by Defendants.

88. As a direct and proximate result of the Data Breach permitted to occur by Defendants, Plaintiff Weigand has suffered, and imminently will suffer, injury-in-fact and damages, including the unauthorized disclosure of the Private Information itself, which, on information and belief due to the nature of the cyberattack, has been or imminently will be posted on the dark web for sale and used for criminal and fraudulent purposes.

89. In addition, as a result of the Data Breach, Plaintiff Weigand has been and will be forced to expend considerable time and effort to monitor her accounts and credit files to protect herself from identity theft and fraudulent misuse of her Private Information disclosed in the Data Breach.

90. Furthermore, Plaintiff Weigand has been caused significant worry and feelings of anxiety and emotional distress regarding the disclosure of her Private Information in the Data

Breach.

91. Had Plaintiff Weigand known that Defendants did not adequately protect her Private Information, she would not have entrusted her sensitive Private Information to Clear Spring or Group 1001.

92. Furthermore, Plaintiffs Weigand's sensitive Private Information remains in Defendants' possession in their computer systems without adequate protection against known threats, exposing her to future breaches and additional harm.

93. As a result of the Data Breach, Plaintiff Weigand faces a lifetime risk of identity theft, as it includes sensitive information that cannot be changed, like her Social Security number. Accordingly, the identity theft protection which Defendants offered is wholly insufficient to compensate her and the Class Members for their damages resulting therefrom.

ii. Plaintiff Cheryl Schmidt

94. Plaintiff Cheryl Schmidt was a customer of Defendants, having purchased an annuity policy from Clear Spring in 2010, and being covered under an annuity with Delaware Life through her husband, Plaintiff Calvin Schmidt..

95. As a condition of receiving Clear Spring's, Delaware Life's and Group 1001's financial services, Plaintiff Cheryl Schmidt was required to provide said Defendants with her Private Information, including but not limited to her name, address, date of birth, Social Security number, and contract/policy number.

96. In entrusting her Private Information to Clear Spring, Delaware Life, and Group 1001, Plaintiff Cheryl Schmidt believed that they would adequately safeguard that information, including as set forth in their privacy policies. Had Plaintiff Cheryl Schmidt known that Clear Spring, Delaware Life, and Group 1001 did not utilize reasonable data security measures, she

would not have entrusted her Private Information to Defendants.

97. Plaintiff Cheryl Schmidt received Clear Spring's Data Breach Notice dated July 28, 2023 in early August 2023, informing her that her Private Information, including her name, address, date of birth, Social Security number, and contract/policy number were unauthorizedly disclosed to and acquired by cybercriminals in Defendants' Data Breach. *See Exhibit C.*

98. As a direct and proximate result of the Data Breach permitted to occur by Defendants, Plaintiff Cheryl Schmidt has suffered, and imminently will suffer, injury-in-fact and damages, including the unauthorized disclosure of the Private Information itself, which, on information and belief due to the nature of the cyberattack, has been or imminently will be posted on the dark web for sale and used for criminal and fraudulent purposes.

99. In addition, as a result of the Data Breach, Plaintiff Cheryl Schmidt has been and will be forced to expend considerable time and effort to monitor her accounts and credit files to protect herself from identity theft and fraudulent misuse of her Private Information disclosed in the Data Breach.

100. Furthermore, Plaintiff Cheryl Schmidt has been caused significant worry and feelings of anxiety and emotional distress regarding the disclosure of her Private Information in the Data Breach.

101. Had Plaintiff Cheryl Schmidt known that Defendants did not adequately protect her Private Information, she would not have entrusted her sensitive Private Information to Clear Spring, Delaware Life, or Group 1001.

102. Furthermore, Plaintiffs Cheryl Schmidt's sensitive Private Information remains in Defendants' possession in their computer systems without adequate protection against known threats, exposing her to future breaches and additional harm.

103. As a result of the Data Breach, Plaintiff Cheryl Schmidt faces a lifetime risk of identity theft, as it includes sensitive information that cannot be changed, like her Social Security number. Accordingly, the identity theft protection which Defendants offered is wholly insufficient to compensate her and the Class Members for their damages resulting therefrom.

iii. Plaintiff Calvin Schmidt

104. Plaintiff Calvin Schmidt was a customer of Defendants, having purchased an annuity policy from Clear Spring in 2019, and in June 2020 for his wife, Plaintiff Cheryl Schmidt, and having purchased an annuity from Delaware Life several years ago.

105. As a condition of receiving Clear Spring's, Delaware Life's and Group 1001's financial services, Plaintiff Calvin Schmidt was required to provide said Defendants with his Private Information, including but not limited to his name, address, date of birth, Social Security number, and contract/policy number.

106. In entrusting his Private Information to Clear Spring, Delaware Life, and Group 1001, Plaintiff Calvin Schmidt believed that they would adequately safeguard that information, including as set forth in their privacy policies. Had Plaintiff Calvin Schmidt known that Clear Spring, Delaware Life, and Group 1001 did not utilize reasonable data security measures, he would not have entrusted her Private Information to Defendants.

107. Plaintiff Calvin Schmidt received Delaware Life's Data Breach Notice dated July 28, 2023 in early August 2023, informing him that his Private Information, including his name, address, date of birth, Social Security number, and contract/policy number were unauthorizedly disclosed to and acquired by cybercriminals in Defendants' Data Breach. *See Exhibit D.*

108. As a direct and proximate result of the Data Breach permitted to occur by Defendants, Plaintiff Calvin Schmidt has suffered, and imminently will suffer, injury-in-fact and

damages, including the unauthorized disclosure of the Private Information itself, which, on information and belief due to the nature of the cyberattack, has been or imminently will be posted on the dark web for sale and used for criminal and fraudulent purposes.

109. In addition, as a result of the Data Breach, Plaintiff Calvin Schmidt has been and will be forced to expend considerable time and effort to monitor his accounts and credit files to protect himself from identity theft and fraudulent misuse of his Private Information disclosed in the Data Breach.

110. Furthermore, Plaintiff Calvin Schmidt has been caused significant worry and feelings of anxiety and emotional distress regarding the disclosure of his Private Information in the Data Breach.

111. Had Plaintiff Calvin Schmidt known that Defendants did not adequately protect his Private Information, he would not have entrusted his sensitive Private Information to Clear Spring, Delaware Life, or Group 1001.

112. Furthermore, Plaintiffs Calvin Schmidt's sensitive Private Information remains in Defendants' possession in their computer systems without adequate protection against known threats, exposing him to future breaches and additional harm.

113. As a result of the Data Breach, Plaintiff Calvin Schmidt faces a lifetime risk of identity theft, as it includes sensitive information that cannot be changed, like his Social Security number. Accordingly, the identity theft protection which Defendants offered is wholly insufficient to compensate her and the Class Members for their damages resulting therefrom.

D. This Data Breach was Foreseeable by Defendants.

114. Plaintiffs and the proposed Class Members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants would

comply with their obligations to keep such information confidential and secure from unauthorized access. By failing to do so, Defendants put all Class Members at risk of identity theft, financial fraud, and other harms.

115. Defendants tortiously failed to take the necessary precautions required to safeguard and protect the Private Information of Plaintiffs and the Class Members from unauthorized disclosure. Defendants' actions represent a flagrant disregard of Plaintiffs' and the other Class Members' rights.

116. Plaintiffs and Class members were the foreseeable and probable victims of Defendants' inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing Private Information and the critical importance of providing adequate security for that information.

117. Cyber-attacks against financial institutions such as Defendants are targeted and frequent. According to Contrast Security's 2023 report, "Cyber Bank Heists: Threats to the financial sector," "[o]ver the past year, attacks have included banking trojans, ransomware, account takeover, theft of customer data and cybercrime cartels deploying 'trojanized' finance apps to deliver malware in spear-phishing campaigns."⁵⁷ In fact, "40% [of financial institutions] have been victimized by a ransomware attack."⁵⁸

118. According to the Identity Theft Resource Center's January 24, 2022 report for 2021, "the overall number of data compromises (1,862) is up more than 68 percent compared to 2020. The new record number of data compromises is 23 percent over the previous all-time high (1,506) set in 2017. The number of data events that involved sensitive information (Ex: Social Security

⁵⁷Contrast Security, "Cyber Bank Heists: Threats to the financial sector," pg. 5, avail. at <https://www.contrastsecurity.com/hubfs/Cyber%20Bank%20Heists%20Report%202023.pdf?hsLang=en> (last acc. Jun 8, 2023).

⁵⁸ *Id.*, pg. 15.

numbers) increased slightly compared to 2020 (83 percent vs. 80 percent).”⁵⁹

119. The increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendants’ industry, including Group 1001, Clear Spring, and Delaware Life. According to IBM’s 2022 report, “[f]or 83% of companies, it’s not if a data breach will happen, but when.”⁶⁰

120. Based on data from the Maine Attorney General, as of August 2022, “...at least 79 financial service companies have reported data breaches affecting 1,000 or more consumers, and the total number of consumers affected by these breaches could be as high as 9.4 million.”⁶¹

121. Private Information/PII is of great value to hackers and cybercriminals, and the data compromised in the Data Breach can be used for a variety of unlawful and nefarious purposes, including ransomware and fraudulent misuse, and sale on the Dark Web,

122. Private Information/PII can be used to distinguish, identify, or trace an individual’s identity, such as their name, Social Security number, and financial records. This can be accomplished alone, or in combination with other personal or identifying information that is connected, or linked to an individual, such as their birthdate, birthplace, and mother’s maiden name.

123. Given the nature of the Data Breach, it was foreseeable that the compromised

⁵⁹ See “Identity Theft Resource Center’s 2021 Annual Data Breach Report Sets New Record for Number of Compromises,” Jan. 24, 2022, available at <https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/> (last acc. Apr. 14, 2023).

⁶⁰ IBM, “Cost of a data breach 2022: A million-dollar race to detect and respond,” available at <https://www.ibm.com/reports/data-breach> (last acc. Apr. 14, 2023).

⁶¹ Carter Pape, “Breach data from Maine shows scope of bank, credit union exposures,” American Banker, August 24, 2022, available at <https://www.americanbanker.com/news/breach-data-from-maine-shows-scope-of-bank-credit-union-exposures>

Private Information/PII could be used by hackers and cybercriminals in a variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiff's and the Class Members' PII can easily obtain their tax returns or open fraudulent credit card accounts in the Class Members' names.

E. Defendants Failed to Comply with FTC Guidelines

124. 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.

125. In 2016, the FTC updated its publication, *Protecting Private Information: A Guide for Business*, which establishes cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of Private 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. 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.⁶²

126. 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

⁶² See Federal Trade Commission, October 2016, "Protecting Private information: A Guide for Business," available at https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf (last acc. Apr. 14, 2023).

reasonable security measures.⁶³

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

128. These FTC enforcement actions include actions against entities failing to safeguard Private Information such as Defendants. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) (“[T]he Commission concludes that LabMD’s data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.”).

129. Defendants failed to properly implement basic data security practices widely known throughout the industry. Defendants’ failures to employ reasonable and appropriate measures to protect against unauthorized access to employee Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

130. Defendants were at all times fully aware of their obligations to protect the Private Information of its current and former customers and/or employees. Defendants were also aware of the significant repercussions that would result from their failure to do so.

F. Defendants Fail to Comply with Industry Standards

131. As shown above, experts studying cyber security routinely identify organizations holding Private Information as being particularly vulnerable to cyber-attacks because of the value

⁶³ *See id.*

of the information they collect and maintain. As of 2022, ransomware breaches like that which occurred here had grown by 41% in the last year and cost on average \$4.54 million dollars.⁶⁴

132. A number of industry and national best practices have been published and are widely used as a go-to resource when developing an institution's cybersecurity standards. The Center for Internet Security's (CIS) CIS Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including 18 Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.⁶⁵

133. In addition, the National Institute of Standards and Technology (NIST) recommends certain practices to safeguard systems, *infra*, such as:

- Control who logs on to your network and uses your computers and other devices.
- Use security software to protect data.
- Encrypt sensitive data, at rest and in transit.
- Conduct regular backups of data.
- Update security software regularly, automating those updates if possible.

⁶⁴ IBM, "Cost of a data breach 2022: A million-dollar race to detect and respond," available at <https://www.ibm.com/reports/data-breach> (last acc. Apr. 14, 2023).

⁶⁵ See <https://www.rapid7.com/solutions/compliance/critical-controls/> (last acc. Apr. 14, 2023).

- Have formal policies for safely disposing of electronic files and old devices.
- Train everyone who uses your computers, devices, and network about cybersecurity. You can help customers understand their personal risk in addition to their crucial role in the workplace.⁶⁶

134. Upon information and belief, Defendants failed to meet the minimum standards of both the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and other industry standards for protecting Plaintiffs' and the proposed Class Members' Private Information—resulting in the Data Breach.

G. The Data Breach Caused Plaintiffs and the Class Members Injury and Damages

135. Plaintiffs and members of the proposed Class have suffered injury and damages from the unauthorized disclosure of their Private Information in the Data Breach that can be directly traced to Defendants' failures to adequately protect that Private Information, that have occurred, are ongoing, and imminently will occur.

136. As stated prior, in the Data Breach, unauthorized cybercriminals were able to access the Plaintiffs' and the proposed Class Members' Private Information, which on information and belief is now being used or will imminently be used for fraudulent purposes and/or has been sold for such purposes and posted on the dark web for sale, causing widespread injury and damages.

137. The ramifications of Defendants' failure to keep Plaintiffs' and the Class's Private Information secure are severe. Identity theft occurs when someone uses another's personal and

⁶⁶ Understanding The NIST Cybersecurity Framework, <https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/nist-framework> (last acc. Apr. 14, 2023).

financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, or other information, such as addresses, without permission, to commit fraud or other crimes.

138. As a direct and proximate result of the Data Breach permitted by Defendants to occur, Plaintiffs and the Class Members have suffered, will imminently suffer, and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. Plaintiffs and the Class Members have suffered, are at an increased risk of suffering, or will imminently suffer:

- a. The loss of the opportunity to control how Private Information is used;
- b. The diminution in value of their Private Information;
- c. The compromise and continuing publication of their Private Information;
- d. Out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;
- f. Delay in receipt of tax refund monies;
- g. Unauthorized use of stolen Private Information; and
- h. The continued risk to their Private Information, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fails to undertake the appropriate measures to protect the Private

Information in its possession.

139. Furthermore, the Data Breach has placed Plaintiffs and the proposed Class Members at an increased risk of fraud and identity theft.

140. There are myriad dangers which affect victims of identity theft, including: cybercriminals opening new financial accounts, credit cards, and loans in victim's names; victim's losing health care benefits (medical identity theft); hackers taking over email and other accounts; time and effort to repair credit scores; losing home due to mortgage and deed fraud; theft of tax refunds; hackers posting embarrassing posts on victim's social media accounts; victims spending large amounts of time and money to recover their identities; experiencing psychological harm and emotional distress; victims becoming further victimized by repeat instances of identity theft and fraud; cybercriminals committing crimes in victim's names; victims' personal data circulating the Dark Web forever; victims receiving increased spam telephone calls and emails; victims' children or elderly parents having their identities stolen.⁶⁷

94. The FTC recommends that identity theft victims take several costly 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 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, seeking a credit freeze, and correcting their credit reports.⁶⁸

95. The time-consuming process recommended by the FTC and other experts is complicated by the vulnerable situations of Defendants' customers.

⁶⁷ See Gaetano DiNardi, Aura.com, "How Bad Is Identity Theft? Is It Serious?" (December 14, 2022) available at <https://www.aura.com/learn/dangers-of-identity-theft#:~:text=Fraudsters%20can%20open%20new%20accounts,to%20repair%20your%20credit%20score> (last acc. Feb. 27, 2023).

⁶⁸ See <https://www.identitytheft.gov/Steps> (last visited [September 1, 2021](#)).

96. Identity thieves use stolen Private Information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

97. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information.

98. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's Private Information to police during an arrest—resulting in an arrest warrant being issued in the victim's name.

99. Further, according to the Identity Theft Resource Center's 2021 Consumer Aftermath Report, identity theft victims suffer “staggering” emotional tolls: For example, nearly 30% of victims have been the victim of a previous identity crime; an all-time high number of victims say they have contemplated suicide. Thirty-three percent reported not having enough money to pay for food and utilities, while 14% were evicted because they couldn't pay rent or their mortgage. Fifty-four percent reported feelings of being violated.⁶⁹

100. What's more, theft of Private Information is also gravely serious outside of the traditional risks of identity theft. In the last two decades, as more and more of our lives become interconnected through the lens of massively complex cloud computing, Private Information is a valuable property right.⁷⁰

⁶⁹ See Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (June 11, 2021), avail. at <https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/> citing Identity Theft Resource Center, “2021 Consumer Aftermath Report,” May 26, 2021 available at <https://www.idtheftcenter.org/post/the-identity-theft-resource-centers-2021-consumer-aftermath-report-reveals-impacts-on-covid-19-identity-crime-victims/> (last acc. Feb. 27, 2023).

⁷⁰ See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The “Value” of Personally*

102. The value of sensitive information is axiomatic; one need only consider the value of Big Data in corporate America, or that the consequences of cyber theft include heavy prison sentences. Even the obvious risk to reward analysis of cybercrime illustrates beyond doubt that Private Information has considerable market value.

103. Theft of Private Information, in particular, is problematic because: “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.”⁷¹

104. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

105. Private Information and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the “cyber black-market” for years.

106. Where the most Private Information belonging to Plaintiffs and Class Members was accessible from Defendants’ network, there is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiffs and the Class Members are at an increased risk of fraud and identity theft for many years into the future.

107. Thus, Plaintiffs and the Class Members must vigilantly monitor their financial and

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).

⁷¹ See *Medical Identity Theft, Federal Trade Commission Consumer Information* (last visited: [June 7, 2022](http://www.consumer.ftc.gov/articles/0171-medical-identity-theft)), <http://www.consumer.ftc.gov/articles/0171-medical-identity-theft>.

medical accounts for many years to come.

108. Social Security numbers are among the worst kinds of Private Information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud.⁷²

109. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.⁷³ Each of these fraudulent activities is difficult to detect. An individual may not know that her or her Social Security number 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.

110. Moreover, it is not an easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as “[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.”⁷⁴

⁷² See U.S. Social Security Administration, “Identity Theft and Your Social Security Number,” Publication No. 05-10064, July 2021, available at <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last acc. Feb. 25, 2023)

⁷³ See *id.*

⁷⁴ *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR, Brian Naylor, Feb. 9, 2015, <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last visited September 1, 2021).

111. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market.”⁷⁵

112. Accordingly, the Data Breach has caused Plaintiffs and the proposed Class Members a greatly increased risk of identity theft and fraud, in addition to the other injuries and damages set forth herein, specifically the imminent identity fraud and criminal fraudulent activity; lost time and efforts in remediating the impact of the Data Breach, and other injury and damages as set forth in the preceding paragraphs.

113. Defendants knew or should have known of these harms which would be caused by the Data Breach it permitted to occur, and strengthened their data systems accordingly.

CLASS ACTION ALLEGATIONS

114. Plaintiffs bring this action on behalf of themselves and as a class action under Rule 23(a) of the Federal Rules of Civil Procedure, and Fed. R. Civ. P. 23(b)(3), on behalf of the following proposed class (“the Class”):

All persons whose Private Information was compromised in Defendants’ Data Breach discovered on February 9, 2023, as announced in their notices in July 2023.

115. Excluded from the Class are Defendants’ officers, directors, and legal representatives and the judges and court personnel in this case and any members of their immediate families.

⁷⁵ *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, Feb. 6, 2015, <http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited September 1, 2021).

116. This action satisfies the requirements for a class action under Fed. R. Civ. P. 23(a)(1)-(3) and Fed. R. Civ. P. 23(b)(3), including requirements of numerosity, commonality, typicality, adequacy, predominance, and superiority.

117. Numerosity. Plaintiffs are representatives of the proposed Class, consisting of over 4,393 individuals, approximately, which are identifiable based on Defendants' records, and far too many to join in a single action.

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

- a. Whether Defendants failed to adopt the practices and procedures necessary to adequately safeguard the information compromised in the Data Breach;
- b. Whether Defendants timely, adequately, and accurately informed Class Members that their Private Information had been compromised;
- c. Whether and to what extent Defendants breached their implied contract with Plaintiffs and the Class;
- d. Whether Defendants were unjustly enriched;
- e. Whether Defendants acted negligently;
- f. Whether Class members are entitled to damages as a result of Defendants' wrongful conduct;
- g. Whether Plaintiffs and the Class are entitled to restitution as a result of Defendants' wrongful conduct; and
- h. Whether Plaintiffs and the Class are entitled to injunctive relief.

119. Typicality. Plaintiffs' claims are typical of those of other Class members because

Plaintiffs' Private Information, like that of every other Class Member, was compromised by the Data Breach. Further, Plaintiffs, like all Class members, were injured by Defendants' uniform misconduct. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of other Class members arise from the same operative facts and are based on the same legal theories.

120. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Class in that they have no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. The damages and infringement of rights Plaintiffs suffered are typical of other Class members, and Plaintiffs seek no relief that is antagonistic or adverse to the members of the Class. Plaintiffs have retained counsel experienced in complex consumer class action litigation, including data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

121. Superiority of Class Action. A class action is superior to other available methods for the fair and efficient adjudication of this controversy, as the pursuit of numerous individual lawsuits would not be economically feasible for individual Class members, and certification as a class action will preserve judicial resources by allowing the Class's common issues to be adjudicated in a single forum, avoiding the need for duplicative hearings and discovery in individual actions that are based on an identical set of facts. In addition, without a class action, it is likely that many members of the Class will remain unaware of the claims they may possess.

122. 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 demonstrates that there would be no significant manageability problems with prosecuting

this lawsuit as a class action.

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

124. Predominance. Pursuant to Fed. R. Civ. 23(b)(3), the issues in this action 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 the questions identified above.

125. This proposed class action does not present any unique management difficulties.

**FIRST CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)**

126. Plaintiffs restate and re-allege all preceding paragraphs as if fully set forth herein.

127. Plaintiffs and Class members were required to provide their Private Information—including their names, addresses, dates of birth, Social Security numbers, and contract/policy numbers and other Private Information—to Defendants as a condition of receiving Clear Spring's, Delaware Life's and Group 1001's financial annuity services, or as a condition of employment.

128. Implicit in the agreement between Defendants and its customers and/or employees was the obligation that the parties would maintain the Private Information confidentially and securely, including those obligations set forth in Defendants' privacy policies to maintain adequate safeguards to safeguard nonpublic Private Information from unauthorized use or improper access, and in their conduct and other representations.

129. Defendants had an implied duty of good faith to ensure that the Private Information of Plaintiffs and Class members in their possession was only used only as authorized, such as to render financial annuity services or as a condition of employment.

130. Defendants had an implied duty to reasonably safeguard and protect the Private Information of Plaintiffs and Class members from unauthorized disclosure or use.

131. Additionally, Defendants implicitly promised to retain this Private Information only under conditions that kept such information secure and confidential.

132. Plaintiffs and Class members fully performed their obligations under the implied contract with Defendants. Defendants did not. Plaintiffs and Class members would not have provided their confidential Private Information to Defendants in the absence of their implied contracts with Defendants and would have instead retained the opportunity to control their Private Information for uses other than Defendants' provision of financial annuity services or as a condition of employment.

133. Defendants breached the implied contracts with Plaintiffs and Class members by failing to reasonably safeguard and protect Plaintiffs and Class members' Private Information, which was compromised as a result of the Data Breach.

134. Defendants' acts and omissions have materially affected the intended purpose of the implied contracts requiring Plaintiffs and Class members to provide their Private Information in exchange for medical treatment and benefits.

135. As a direct and proximate result of Defendants' breach of its implied contracts with Plaintiffs and Class members, Plaintiffs and Class members have suffered and will imminently suffer injury, including but not limited to: the loss of the opportunity to control how Private Information is used; diminution in value of their Private Information; the compromise and continuing publication of their Private Information; out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the

actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; delay in receipt of tax refund monies; unauthorized use of stolen Private Information; and the continued risk to their Private Information, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the Private Information in their possession.

**SECOND CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)**

136. Plaintiffs restate and re-allege all preceding paragraphs as if fully set forth herein.

137. This claim is pleaded solely in the alternative to Plaintiffs' implied contract claims.

138. Plaintiffs and Class Members conferred a monetary benefit upon Defendants in the form of monies paid for financial annuity services, and labor rendered in connection with employment.

139. Defendants appreciated or had knowledge of the benefits conferred upon it by Plaintiffs and Class Members.

140. Defendants also benefited from the receipt of Plaintiffs and Class members' Private Information, as this was used to facilitate the provision of financial annuity services and employment.

141. As a result of Defendants' conduct, Plaintiffs and Class Members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiffs and Class members paid for, or the value of labor rendered, and those without reasonable data privacy and security practices and procedures that they received.

142. Under principals of equity and good conscience, Defendants should not be permitted to retain the money or value of labor belonging to Plaintiffs and Class Members because Defendants failed to implement (or adequately implement) the data privacy and security practices and procedures for which Plaintiffs and Class Members paid, and which were otherwise mandated by federal, state, and local laws and by industry standards.

143. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class members all unlawful or inequitable proceeds it received as a result of its conduct and the Data Breach alleged herein.

**THIRD CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)**

144. Plaintiffs restate and re-allege all preceding paragraphs as if fully set forth herein.

145. Upon agreeing to receive financial annuity services from Defendants or as a condition of employment, Plaintiffs and Class Members were obligated to provide Defendants with certain Private Information, including their names, addresses, dates of birth, Social Security numbers, and contract/policy numbers and other Private Information.

146. 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 their Private Information were wrongfully disclosed.

147. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' policies regarding the storage, utilization, and distribution of customers' and employees' Private Information to ensure that Plaintiffs' and Class Members' Private Information

was adequately secured and protected, including in accordance with industry standards and applicable law.

148. Private Information is highly valuable, and Defendants knew or should have known the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiffs and the Class as well as the importance of exercising reasonable care in handling it.

149. The risk that unauthorized persons would try to gain access and misuse to the Private Information stored on Defendants' systems was foreseeable.

150. Defendants had a duty of care to Plaintiffs and Class Members because it was foreseeable that Defendants' failures to adequately safeguard their Private Information in accordance with state-of-the-art industry standards for data security would result in the compromise of that Private Information —just like the Data Breach that ultimately came to pass. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class Members' Private Information by disclosing and allowing access to Private Information to unknown third parties and by failing to properly supervise both the way the Private Information was stored, used, and exchanged, and those in its employ who were responsible for data security.

151. Defendants owed Plaintiffs and Class Members a duty to notify them within a reasonable time frame of any breach to the security of their Private Information. Defendants also owed Plaintiffs and Class members a duty to timely and accurately disclose to them the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and Class members to take appropriate measures to protect their Private Information, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

152. Plaintiffs and Class members 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 Private Information and the critical importance of providing adequate security for that Private Information. Defendants also knew or should have known that it had inadequate employee training and education and information security protocols in place to secure the Private Information of Plaintiffs and the Class.

153. Defendants' conduct created a foreseeable risk of harm to Plaintiffs and Class Members.

154. Defendants' misconduct included, but was not limited to, its failure to take the steps necessary to prevent the Data Breach as set forth herein. Defendants' misconduct also included their decision not to comply with industry standards for the safekeeping and use of the Private Information of Plaintiffs and Class Members.

155. Plaintiffs and Class Members had no ability to protect their Private Information that was in Defendants' possession. Only Defendants were able to protect against the harm Plaintiffs and Class members suffered as a result of the Data Breach.

156. Defendants had and continue to have a duty to adequately notify Plaintiffs and Class Members that their Private Information was compromised, how it was compromised, and other details of the Data Breach. Such notice is necessary to allow Plaintiffs and the Class members to take steps to prevent, mitigate, and repair any identity theft or fraudulent use of their Private Information by unauthorized third parties.

157. Defendants has failed to timely or adequately notify Plaintiffs and the Class of the Data Breach, as the Data Breach Notice(s) did not contain sufficient information detailing the incident, including, but not limited to, key information regarding the nature of the

hacking/ransomware attack and how the unauthorized third party obtained access to Plaintiffs and Class members' Private Information. Defendants' failures to provide appropriate notice of the Data Breach to Plaintiffs and Class members actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and Class members' injuries in fact.

158. Defendants had a duty to have appropriate procedures in place to prevent the unauthorized dissemination of the Private Information of Plaintiffs and Class Members.

159. Defendants have admitted that the privacy and security of Plaintiffs' and Class members' Private Information was compromised as a result of the Data Breach.

160. Defendants, through their acts and/or omissions, unlawfully breached their respective duties to Plaintiffs and the Class by failing to exercise reasonable care in protecting and safeguarding their Private Information.

161. Defendants deviated from standard industry rules, regulations, and practices at the time of the Data Breach by improperly and inadequately safeguarding the Plaintiffs' and Class Members' Private Information.

162. Defendants, through their acts and/or omissions, unlawfully breached their duties to Plaintiffs and the Class by failing to have appropriate procedures in place to store and access customers' and/or employees' Private Information and to detect and prevent unauthorized access to their Private Information.

163. Defendants, through their acts and/or omissions, unlawfully breached their duties to timely and adequately disclose to Plaintiffs and Class members the existence and scope of the Data Breach.

164. But for Defendants' wrongful and negligent breach of these duties, Plaintiffs and Class Members' Private Information would not have been compromised.

165. There is a close causal connection between Defendants' failures to implement security measures to protect the Private Information entrusted to them and the risk of imminent harm suffered by Plaintiffs and the Class.

166. As a result of Defendants' negligence, Plaintiffs and the Class Members have suffered and will imminently suffer injury, including but not limited to: the loss of the opportunity to control how Private Information is used; diminution in value of their Private Information; the compromise and continuing publication of their Private Information; out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; delay in receipt of tax refund monies; unauthorized use of stolen Private Information; and the continued risk to their Private Information, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the Private Information in their possession.

**FOURTH CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)**

167. Plaintiffs restate and re-allege all preceding paragraphs as if fully set forth herein.

168. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' Private Information.

169. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiffs and Class Members' sensitive Private

Information. Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect customers or, in this case, fund participants and customers’ Private Information.

170. Defendants violated their duties under Section 5 of the FTC Act by failing to use reasonable measures to protect their customers’ and employees’ 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 Defendants had collected and stored and the foreseeable consequences of a data breach, including the immense damages that would result to its customers and employees in the event of a breach, which ultimately came to pass.

171. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

172. Defendants had a duty to Plaintiffs and the Class to implement and maintain reasonable security procedures and practices to safeguard their Private Information.

173. Defendants breached their duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs’ and Class members’ Private Information.

174. Defendants’ violations of Section 5 of the FTC Act and their failures to comply with applicable laws and regulations constitute negligence *per se*.

175. But for Defendants’ wrongful and negligent breach of the duties owed to Plaintiffs

and Class Members, Plaintiffs and Class Members would not have been injured.

176. The injury and harm suffered by Plaintiffs and Class Members were the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties and that their breach would cause Plaintiffs and the Class to suffer the foreseeable harms associated with the exposure of their Private Information.

177. Had Plaintiffs and Class Members known that Defendants did not adequately protect the Private Information entrusted to them, Plaintiffs and Class Members would not have entrusted Defendants with their Private Information.

178. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class Members have suffered and will imminently suffer injury, including but not limited to: the loss of the opportunity to control how Private Information is used; diminution in value of their Private Information; the compromise and continuing publication of their Private Information; out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud; lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud; delay in receipt of tax refund monies; unauthorized use of stolen Private Information; and the continued risk to their Private Information, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the Private Information in their possession.

**FIFTH CAUSE OF ACTION
INVASION OF PRIVACY
(On Behalf of Plaintiffs and the Class)**

179. Plaintiffs restate and re-allege all preceding paragraphs as if fully set forth herein.

180. Indiana recognizes the Restatement (Second) of Torts formulation of invasion of privacy, consisting of the distinct injuries: (1) intrusion upon seclusion; (2) appropriation of likeness; (3) public disclosure of private facts; and (4) false light publicity. Herein, Plaintiffs proceed upon the third injury—public disclosure of private facts.

181. Plaintiffs' and Class Members' Private Information is private in nature.

182. Defendants disclosed Plaintiffs' and Class Members' Private Information to the public via the Data Breach, as on information and belief the information has been publicized it on the Dark Web and elsewhere for criminal and fraudulent purposes.

183. The disclosure of Plaintiffs' and Class Members' Private Information, including Social Security numbers would be highly offensive to a reasonable person.

184. The Private Information is not of legitimate public concern.

185. As a direct and proximate result of Defendants' actions alleged above, Plaintiffs and Class Members have suffered damages.

PRAYER FOR RELIEF

WHEREFORE Plaintiffs, CAREY WEIGAND, CHERYL SCHMIDT and CALVIN SCHMIDT, on behalf of themselves and all others similarly situated, request the following relief:

- A. An Order certifying this action as a class action and appointing Plaintiffs as Class representatives and the undersigned as Class counsel;
- B. An award of compensatory and actual damages, as well as punitive damages, in an amount to be determined;
- C. A mandatory injunction directing Defendants to adequately safeguard the Private Information of Plaintiffs and the Class hereinafter by implementing improved security procedures and measures;

- D. A mandatory injunction requiring that Defendants provide notice to each member of the Class relating to the full nature and extent of the Data Breach and the disclosure of Private Information to unauthorized persons;
- E. An award of attorneys' fees and costs;
- F. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law; and
- G. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury under Fed. R. Civ. Proc. 38(b) on all claims so triable.

Dated: August 16, 2023

Respectfully submitted,

s/ Lynn A. Toops

Lynn A. Toops (No. 26386-49)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, IN 46204
(317) 636-6481
(317) 636-2593 (facsimile)
ltoops@cohenandmalad.com

Counsel for the Plaintiffs and the Proposed Class



All News

GROUP1001

Mar 1, 2023 Corporate

Corporate

Community

Sponsorship

Work Life

Media Inquiries

Group 1001 Resumes Full Operations After Ransomware Attack

Group 1001, Inc. would like to provide an update to our stakeholders concerning recent system interruptions experienced by certain Group 1001 Insurance member companies, including Delaware Life Insurance Company, Delaware Life Insurance Company of New York, Clear Spring Life and Annuity Company, Clear Spring Property and Casualty Company, and our Clear Spring Health business. We are pleased to report that all of our companies are back to full functionality.

Incident Overview

- Beginning on February 9, 2023, we were alerted to the existence of sophisticated ransomware on our information technology infrastructure.

- We immediately launched an investigation to determine the full scope of the incident, and a team of third-party forensic experts was engaged to assist in the investigation, which is ongoing.

- Based on our investigation to date, our forensic experts have confirmed that the ransomware code deployed in our environment has been contained and will not spread to any other internal or external systems.

- We have alerted the FBI and will continue to provide information regarding the incident as they investigate.

- We did not pay a ransom.

Exhibit A



Containment & Remediation

All News

Corporate

Community

Sponsorship

Work Life

Media Inquiries

- We took immediate action by proactively disconnecting systems from our network to contain the threat and prevent additional systems from being affected.

- Along with our forensics experts, our team scanned systems for indicators of compromise and remediated any identified indicators of compromise.

- In addition, we deployed additional advanced endpoint detection and monitoring tools on our newly restored systems for an added layer of security and visibility across our network.

- All systems were validated as clean by conducting additional scans before they were brought back online.

- We have been, and continue to be, in communication with our regulators about this incident.

- There will be a number of other infrastructure enhancements to continuously strengthen the security posture of Group 1001's network and systems in the days, months, and years ahead.

Restoration

- While our investigation is ongoing, we are confident that the attack has now been successfully contained.

- We have fully resumed normal operations.

- The security of our information and that of our contract holders and other stakeholders is important to us. Once our investigation is complete, we will notify any impacted parties as appropriate.

We want to confirm that it is safe to conduct business with us and to communicate with us via e-mail, our website portals, and our call centers. We apologize for any inconvenience and genuinely appreciate your patience and understanding as we worked vigorously to fully restore our computer networks.



For further questions about this incident, please e-mail our incident response team at: incidentresponse@group1001.com

All News

Corporate

Community

Sponsorship

Work Life

Media Inquiries

What are you looking for?

Aug 15, 2022 - Aug 15, 2023

GROUP1001

Jul 28, 2023 Corporate

Group 1001 Update on Ransomware Attack

Group 1001, Inc. would like to provide an update to our stakeholders concerning the February 9, 2023, ransomware attack on our information technology infrastructure.

As previously reported, we immediately launched an investigation to determine the full scope of the incident, and a team of leading third-party forensic e...



All News

Corporate

Community

Sponsorship

Work Life

Media Inquiries



Jul 27, 2023 Corporate

Group 1001 Appreciates Our 2023 Summer Interns

We are excited to work with 11 summer interns! Group 1001's internships are designed to provide a highly engaging, real-life experience where students have the opportunity to work on real projects, make an impact, and gain valuable business skills.

"Group 1001 is committed to providing interns the opportunity to provide..."

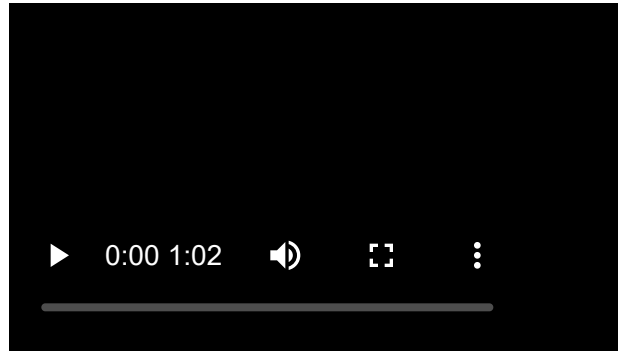


Jul 12, 2023 Corporate

Delaware Life Insurance Company Recognized as a 2023 Ward's Top 50 Life-Health Company

Delaware Life Insurance Company, a Group 1001 Company, has been recognized as a top-performing

company in the insurance industry by Ward, an Aon company, who is a leading benchmarking provider for the insurance industry. This prestigious group of 50 companies is chosen based on publicly available data to identify the t...



Jun 28, 2023 Corporate

Group 1001 Honored with HR Impact Award from Indianapolis Business Journal

Group 1001 received an **HR Impact Award** presented by the Indianapolis Business Journal! The company was recognized in the “employee experience” category, which acknowledges programs and efforts that make an organization a better place to work, whether that’s through strong benefits programs, work/life balance efforts, c...



All News

Corporate

Community

Sponsorship

Work Life

Media Inquiries



Jun 21, 2023 Corporate

Gainbridge®, a Group 1001 Company, Announces Vice President of Marketing, Adam Harrington

Zionsville, IN (June 21, 2023) – Gainbridge®, a Group 1001 company, announced the appointment of Adam Harrington to the position of Vice President of Marketing. With more than 13 years of experience leading customer growth and helping companies elevate their marketing, Harrington will use his extensive background to le...



Jun 14, 2023 Corporate

Group 1001 CEO & President Dan Towriss Speaks at the Marketing Innovation Summit Hosted by Eli Lilly

All News

Corporate

Community

Sponsorship

Work Life

Media Inquiries

CEO and President Dan Towriss spoke at the Marketing Innovation Summit: Driving Brand Purpose, hosted by Eli Lilly and Company on May 25. Towriss presented “Why Motorsports” just prior to the Indy500 race presented by Gainbridge®. The summit featured thought leaders in the industry from companies including PepsiCo, Dom...



Jun 2, 2023 Corporate

Gainbridge’s® Santiago Jeyaseelan Discusses Niche Financial Services for Forbes Technology Council

Santiago Vinoth Jeyaseelan is the VP of Product Management & Design for Gainbridge®. As a Forbes Technology Council member, he talks about the rapidly-evolving state of financial services. Jeyaseelan expands on the rise of embedded finance, the next wave, challenges ahead, and how embedded finance is “reshaping the...

➤ GAINBRIDGE

Jun 1, 2023 Corporate

Gainbridge® Launches New Annuity Product Focused on Flexibility and Risk Mitigation

Zionsville, Indiana (June 1, 2023) – Zionsville, Indiana – Gainbridge Insurance Agency, LLC (“Gainbridge”), a Group 1001 company, is pleased to announce the launch of OneUp™, a new registered index-linked annuity issued by Gainbridge Life Insurance Company through the Gainbridge® platform. The OneUp™ product is current...



May 25, 2023 Corporate

Delaware Life Executives Participate in Association of

GROUP1001

All News

Corporate

Community

Sponsorship

Work Life

Media Inquiries

Life Insurance Counsel's

Delaware Life's Chief Legal Officer, Mike Bloom, and Vice President and Associate General Counsel, Maura Murphy, attended the

Association of Life Insurance Counsel's 2023 Annual Meeting in California on May 7-9. Their participation at the conference exemplified Delaware Life's commitment to staying ahead of the curve, ...

➤ GAINBRIDGE

May 25, 2023 Corporate

Gainbridge Announces Launch of Its New B2B Insurance-as-a-Service Platform and Partnership With SAVE

Zionsville, IN (May 25, 2023) – Gainbridge Insurance Agency, LLC (“Gainbridge”), a Group 1001 company, announced today the upcoming launch of its business-to-business (B2B) “insurance-as-a-service” platform targeting leading financial technology companies with turnkey, intuitive savings, and retirement solutions for th...



All News

Corporate

Community

Sponsorship

Work Life

Media Inquiries



May 18, 2023 Corporate

Parity Appoints Leela Srinivasan as CEO

A seasoned executive and three-time CMO of high-growth companies joins to lead Parity through its next phase.

Parity, and its parent company Group 1001, announced the hiring of Leela Srinivasan as its chief executive officer. Srinivasan, an experienced executive whose 25-year career has spanned roles in marketing, sale...



Mar 2, 2023 Corporate

AM Best Comments on Credit Ratings of Certain Group 1001

GROUP1001

All News

Corporate

Community

Sponsorship

Work Life

Media Inquiries

Insurance Holdings, LLC Subsidiaries Following Ransomware Attack

AM Best has commented that the Credit Ratings (ratings) of certain Group 1001 Insurance Holdings, LLC's rated subsidiaries remain unchanged following the parent company's disclosure that it sustained a cybersecurity attack that caused a network disruption and impacted certain systems.

According to the company, the follo...



a **GROUP1001** company

Nov 4, 2022 Corporate

Barron's Honors Delaware Life for Top-Ranked Annuities for Third Consecutive Year

Delaware Life, a Group 1001 company, has been recognized in a recent Barron's article, "The Best Annuities for Income and Growth." Noting that sales of these investment products have surged this year, the article highlights Delaware Life's Growth Pathway®Fixed Index Annuity and Apex MYGA®Fixed Annuity as standouts in t...

All News

Corporate

Community

Sponsorship

Work Life

Media Inquiries



a **GROUP1001** company

Sep 21, 2022 Corporate

Delaware Life Supports Renewable Energy Projects by Providing \$400 Million Credit Facility to Fundamental Renewables

Delaware Life, acting as arranger and a lead lender, recently provided a \$400 million credit facility to Fundamental Renewables, an established provider of financing for solar and other renewable energy projects. This landmark transaction is an example of an important element of Delaware Life's investment strategy – to...



Aug 22, 2022 Corporate



All News

Corporate

Community

Sponsorship

Work Life

Media Inquiries

Mike Nichols Joins Group 1001 as Chief of Sponsorship Strategy and Activations

Indianapolis, IN (August 22, 2022) – Group 1001 today announced the appointment of Mike Nichols as Chief of Sponsorship Strategy and Activations. Nichols has more than 25 years of executive experience in sports leadership and sponsorships, including more than 16 years at the LPGA (Ladies Professional Golf Association)...

All News

Corporate

Community

Sponsorship

Work Life

Media Inquiries



Aug 15, 2022 Corporate

Introducing Clear Spring Life and Annuity Company

We are pleased to announce Guggenheim Life and Annuity Company, who recently received an upgrade from A.M. Best to a Financial Strength Rating of A- (Excellent), has a new name: Clear Spring Life and Annuity Company ("Clear Spring Life"). In addition, GL Marketing, LLC is now Clear Spring Life Marketing, LLC ("CSL Mark...



©2022 Group 1001. All Rights Reserved. Term & Conditions | Privacy Policy



P.O. Box 989728
West Sacramento, CA 95798-9728

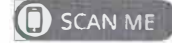


Cary Weigand
[Redacted]
Bandon, OR 97411-6300



Enrollment Code: RFN9EY6WX9

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

July 28, 2023

Notice of Data Breach

Dear Cary Weigand,

We are writing to inform you of an incident that may have affected your personal information and are providing you with information on additional steps you can consider taking to protect your personal information.

You are receiving this notice because you are, or previously were, associated with an annuity contract or life insurance policy issued by our company, Clear Spring Life and Annuity Company (formerly Guggenheim Life and Annuity Company).

What Happened

On February 9, 2023, we were alerted to the existence of sophisticated ransomware on our information technology infrastructure. We immediately took steps to isolate and secure our systems and investigate the incident. We retained a leading third-party forensics firm to conduct a thorough investigation, secure our systems, remediate any risks, and methodically bring our systems back online once such systems were validated as clean. We also alerted appropriate regulatory authorities and the Federal Bureau of Investigation.

As part of our investigation, we determined that an unauthorized malicious actor accessed and acquired certain files from our systems. We have been analyzing the impacted files to understand what personal information may be at risk. The process of locating personal information in the acquired files and matching that information to individuals was complex. This work was substantially completed on July 10, 2023. We then began notifying the individuals whose personal information we believe to have been included, including you.

What Information Was Involved

The type of personal information at risk differs from individual to individual but may have included the following information relating to you: name, address, date of birth, Social Security number, and contract/policy number.

What We Are Doing

Together with our forensics experts, our team scanned our systems for, and remediated, any identified indicators of compromise. Out of an abundance of caution, we have deployed additional advanced endpoint detection and monitoring tools on our newly restored systems for an added layer of security and visibility across our network. We will also continue to make infrastructure enhancements to strengthen and harden the security posture of our network and systems in the days, months, and years ahead.

Exhibit B

In addition, we are offering you identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. The IDX identity protection package includes: Experian, Equifax, and TransUnion credit monitoring, CyberScan™ dark web monitoring, identity theft insurance (for up to \$1,000,000 with no deductible), and fully managed identity restoration services. In some states, these services are required by law. We are offering these services to all affected individuals free of charge for 24 months, regardless of their state of residence.

What You Can Do

We encourage you to enroll and contact IDX with any questions. To enroll in the free identity protection services, please scan the QR code on the first page, or call 1-888-331-6462 or go to <https://app.idx.us/account-creation/protect> and use the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is October 28, 2023.

Once you enroll in these identity protection services, IDX will help you resolve issues if you determine your identity is compromised. To receive the credit monitoring services, you must be over the age of 18, have established credit in the United States, have a Social Security number in your name, and have a U.S. residential address associated with your credit file. If you do not have a credit file or are under the age of 18, you will not be able to register for the credit monitoring services, but you will receive CyberScan™ dark web monitoring, identity theft insurance, and the fully managed identity restoration services from IDX.

Although we have not identified any suspicious activity pertaining to your associated annuity contract or life insurance policy and have not received any reports of misuse of your information, it is always a good practice to be vigilant and closely review and monitor your financial accounts, statements, credit reports, and other financial information for any evidence of unusual activity, fraudulent charges, or signs of identity theft.

IDX representatives have been fully informed regarding the incident and are ready to answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed "Additional Steps You Can Take" document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-888-331-6462 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,



Robert Stanton
Chief Operating Officer

(Enclosure)



Additional Steps You Can Take

- 1. Website and Enrollment.** Scan the QR code or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your unique Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
- 3. Telephone.** Contact IDX at 1-888-331-6462 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
- 4. Review your credit reports.** It is always advisable to remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify IDX immediately by calling or by logging into the IDX website and filing a request for help. If you file a request for help or report suspicious activity, you will be contacted by a member of IDX's ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, IDX will assign you an ID Care Specialist who will work on your behalf.

You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General of your state.

5. Place Fraud Alerts with any of the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will

need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer credit reporting agencies by regular, certified, or overnight mail at the addresses below or, if available, comply with the consumer credit reporting agencies' online security freeze request procedures:

Equifax Security Freeze
1-888-298-0045
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
www.transunion.com
P.O. Box 160
Woodlyn, PA 19094

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past 5 years, provide the addresses where you have lived over the prior 5 years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have 3 business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to you within 5 days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual to access your credit report, you must call or send a written request to the credit reporting agencies by mail, or, if available, comply with the credit reporting agencies' online procedures for lifting a security freeze and provide proper identification (name, address, and Social Security number), and the PIN or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report, or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receipt of your request to lift the security freeze as requested.

To remove the security freeze, you must send a written request to each of the credit reporting agencies by mail or, if available, comply with the credit reporting agencies' online procedures for removing a security freeze. The credit reporting agencies have 3 business days after receipt of your request to remove the security freeze.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The **Federal Trade Commission** also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's office to report suspected incidents of identity theft at Iowa Attorney General's Office, Director of Consumer Protection Division, 1305 E. Walnut Street, Des Moines, IA 50319, 1-515-281-5926, www.iowaattorneygeneral.gov.



Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. See **Section 6** for information on how to place a security freeze on your credit report.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting and Identity Security Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting and Identity Security Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting and Identity Security Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting and Identity Security Act. You can review your rights pursuant to the Fair Credit Reporting and Identity Security Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-877-566-7226 (toll free within North Carolina) or 601-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. There were 268 Rhode Island residents impacted by the incident. Under Rhode Island law, you have the right to obtain any police report filed in regard to the incident.

All U.S. Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.



P.O. Box 989728
West Sacramento, CA 95798-9728



Cheryl Schmidt
[Redacted]
Cold Spring, MN 56320-4512



Enrollment Code: AGY3XTVKT3

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

July 28, 2023

Notice of Data Breach

Dear Cheryl Schmidt,

We are writing to inform you of an incident that may have affected your personal information and are providing you with information on additional steps you can consider taking to protect your personal information.

You are receiving this notice because you are, or previously were, associated with an annuity contract or life insurance policy issued by our company, Clear Spring Life and Annuity Company (formerly Guggenheim Life and Annuity Company).

What Happened

On February 9, 2023, we were alerted to the existence of sophisticated ransomware on our information technology infrastructure. We immediately took steps to isolate and secure our systems and investigate the incident. We retained a leading third-party forensics firm to conduct a thorough investigation, secure our systems, remediate any risks, and methodically bring our systems back online once such systems were validated as clean. We also alerted appropriate regulatory authorities and the Federal Bureau of Investigation.

As part of our investigation, we determined that an unauthorized malicious actor accessed and acquired certain files from our systems. We have been analyzing the impacted files to understand what personal information may be at risk. The process of locating personal information in the acquired files and matching that information to individuals was complex. This work was substantially completed on July 10, 2023. We then began notifying the individuals whose personal information we believe to have been included, including you.

What Information Was Involved

The type of personal information at risk differs from individual to individual but may have included the following information relating to you: name, address, date of birth, Social Security number, and contract/policy number.

What We Are Doing

Together with our forensics experts, our team scanned our systems for, and remediated, any identified indicators of compromise. Out of an abundance of caution, we have deployed additional advanced endpoint detection and monitoring tools on our newly restored systems for an added layer of security and visibility across our network. We will also continue to make infrastructure enhancements to strengthen and harden the security posture of our network and systems in the days, months, and years ahead.

Exhibit C

In addition, we are offering you identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. The IDX identity protection package includes: Experian, Equifax, and TransUnion credit monitoring, CyberScan™ dark web monitoring, identity theft insurance (for up to \$1,000,000 with no deductible), and fully managed identity restoration services. In some states, these services are required by law. We are offering these services to all affected individuals free of charge for 24 months, regardless of their state of residence.

What You Can Do

We encourage you to enroll and contact IDX with any questions. To enroll in the free identity protection services, please scan the QR code on the first page, or call 1-888-331-6462 or go to <https://app.idx.us/account-creation/protect> and use the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is October 28, 2023.

Once you enroll in these identity protection services, IDX will help you resolve issues if you determine your identity is compromised. To receive the credit monitoring services, you must be over the age of 18, have established credit in the United States, have a Social Security number in your name, and have a U.S. residential address associated with your credit file. If you do not have a credit file or are under the age of 18, you will not be able to register for the credit monitoring services, but you will receive CyberScan™ dark web monitoring, identity theft insurance, and the fully managed identity restoration services from IDX.

Although we have not identified any suspicious activity pertaining to your associated annuity contract or life insurance policy and have not received any reports of misuse of your information, it is always a good practice to be vigilant and closely review and monitor your financial accounts, statements, credit reports, and other financial information for any evidence of unusual activity, fraudulent charges, or signs of identity theft.

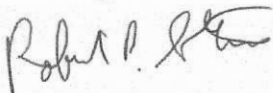
IDX representatives have been fully informed regarding the incident and are ready to answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed "Additional Steps You Can Take" document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-888-331-6462 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,



Robert Stanton
Chief Operating Officer

(Enclosure)



Additional Steps You Can Take

1. **Website and Enrollment.** Scan the QR code or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your unique Enrollment Code provided at the top of the letter.
2. **Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
3. **Telephone.** Contact IDX at 1-888-331-6462 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
4. **Review your credit reports.** It is always advisable to remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify IDX immediately by calling or by logging into the IDX website and filing a request for help. If you file a request for help or report suspicious activity, you will be contacted by a member of IDX's ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, IDX will assign you an ID Care Specialist who will work on your behalf.

You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General of your state.

5. **Place Fraud Alerts** with any of the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. **Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will

need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer credit reporting agencies by regular, certified, or overnight mail at the addresses below or, if available, comply with the consumer credit reporting agencies' online security freeze request procedures:

Equifax Security Freeze
1-888-298-0045
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
www.transunion.com
P.O. Box 160
Woodlyn, PA 19094

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past 5 years, provide the addresses where you have lived over the prior 5 years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have 3 business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to you within 5 days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual to access your credit report, you must call or send a written request to the credit reporting agencies by mail, or, if available, comply with the credit reporting agencies' online procedures for lifting a security freeze and provide proper identification (name, address, and Social Security number), and the PIN or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report, or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receipt of your request to lift the security freeze as requested.

To remove the security freeze, you must send a written request to each of the credit reporting agencies by mail or, if available, comply with the credit reporting agencies' online procedures for removing a security freeze. The credit reporting agencies have 3 business days after receipt of your request to remove the security freeze.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The **Federal Trade Commission** also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's office to report suspected incidents of identity theft at Iowa Attorney General's Office, Director of Consumer Protection Division, 1305 E. Walnut Street, Des Moines, IA 50319, 1-515-281-5926, www.iowaattorneygeneral.gov.



Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. See **Section 6** for information on how to place a security freeze on your credit report.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting and Identity Security Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting and Identity Security Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting and Identity Security Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting and Identity Security Act. You can review your rights pursuant to the Fair Credit Reporting and Identity Security Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fera.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-877-566-7226 (toll free within North Carolina) or 601-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. There were 268 Rhode Island residents impacted by the incident. Under Rhode Island law, you have the right to obtain any police report filed in regard to the incident.

All U.S. Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.



P.O. Box 989728
West Sacramento, CA 95798-9728



Calvin Schmidt

[Redacted]
Cold Spring, MN 56320-4512



Enrollment Code: EGGZJWFF9S

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

July 28, 2023

Notice of Data Breach

Dear Calvin Schmidt,

We are writing to inform you of an incident that may have affected your personal information and are providing you with information on additional steps you can consider taking to protect your personal information.

You are receiving this notice because you are, or previously were, associated with an annuity contract or life insurance policy issued by our company, Delaware Life Insurance Company.

What Happened

On February 9, 2023, we were alerted to the existence of sophisticated ransomware on our information technology infrastructure. We immediately took steps to isolate and secure our systems and investigate the incident. We retained a leading third-party forensics firm to conduct a thorough investigation, secure our systems, remediate any risks, and methodically bring our systems back online once such systems were validated as clean. We also alerted appropriate regulatory authorities and the Federal Bureau of Investigation.

As part of our investigation, we determined that an unauthorized malicious actor accessed and acquired certain files from our systems. We have been analyzing the impacted files to understand what personal information may be at risk. The process of locating personal information in the acquired files and matching that information to individuals was complex. This work was substantially completed on July 10, 2023. We then began notifying the individuals whose personal information we believe to have been included, including you.

What Information Was Involved

The type of personal information at risk differs from individual to individual but may have included the following information relating to you: name, address, date of birth, Social Security number, and contract/policy number.

What We Are Doing

Together with our forensics experts, our team scanned our systems for, and remediated, any identified indicators of compromise. Out of an abundance of caution, we have deployed additional advanced endpoint detection and monitoring tools on our newly restored systems for an added layer of security and visibility across our network. We will also continue to make infrastructure enhancements to strengthen and harden the security posture of our network and systems in the days, months, and years ahead.

Exhibit D

In addition, we are offering you identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. The IDX identity protection package includes: Experian, Equifax, and TransUnion credit monitoring, CyberScan™ dark web monitoring, identity theft insurance (for up to \$1,000,000 with no deductible), and fully managed identity restoration services. In some states, these services are required by law. We are offering these services to all affected individuals free of charge for 24 months, regardless of their state of residence.

What You Can Do

We encourage you to enroll and contact IDX with any questions. To enroll in the free identity protection services, please scan the QR code on the first page, or call 1-888-331-6462 or go to <https://app.idx.us/account-creation/protect> and use the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is October 28, 2023.

Once you enroll in these identity protection services, IDX will help you resolve issues if you determine your identity is compromised. To receive the credit monitoring services, you must be over the age of 18, have established credit in the United States, have a Social Security number in your name, and have a U.S. residential address associated with your credit file. If you do not have a credit file or are under the age of 18, you will not be able to register for the credit monitoring services, but you will receive CyberScan™ dark web monitoring, identity theft insurance, and the fully managed identity restoration services from IDX.

Although we have not identified any suspicious activity pertaining to your associated annuity contract or life insurance policy and have not received any reports of misuse of your information, it is always a good practice to be vigilant and closely review and monitor your financial accounts, statements, credit reports, and other financial information for any evidence of unusual activity, fraudulent charges, or signs of identity theft.

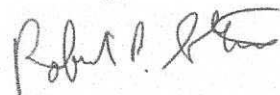
IDX representatives have been fully informed regarding the incident and are ready to answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed "Additional Steps You Can Take" document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-888-331-6462 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,



Robert Stanton
Chief Operating Officer

(Enclosure)



Additional Steps You Can Take

- 1. Website and Enrollment.** Scan the QR code or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your unique Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
- 3. Telephone.** Contact IDX at 1-888-331-6462 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
- 4. Review your credit reports.** It is always advisable to remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify IDX immediately by calling or by logging into the IDX website and filing a request for help. If you file a request for help or report suspicious activity, you will be contacted by a member of IDX's ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, IDX will assign you an ID Care Specialist who will work on your behalf.

You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General of your state.

- 5. Place Fraud Alerts** with any of the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

- 6. Security Freeze.** By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will

need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer credit reporting agencies by regular, certified, or overnight mail at the addresses below or, if available, comply with the consumer credit reporting agencies' online security freeze request procedures:

Equifax Security Freeze
1-888-298-0045
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
www.transunion.com
P.O. Box 160
Woodlyn, PA 19094

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past 5 years, provide the addresses where you have lived over the prior 5 years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have 3 business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to you within 5 days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual to access your credit report, you must call or send a written request to the credit reporting agencies by mail, or, if available, comply with the credit reporting agencies' online procedures for lifting a security freeze and provide proper identification (name, address, and Social Security number), and the PIN or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report, or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receipt of your request to lift the security freeze as requested.

To remove the security freeze, you must send a written request to each of the credit reporting agencies by mail or, if available, comply with the credit reporting agencies' online procedures for removing a security freeze. The credit reporting agencies have 3 business days after receipt of your request to remove the security freeze.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The **Federal Trade Commission** also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's office to report suspected incidents of identity theft at Iowa Attorney General's Office, Director of Consumer Protection Division, 1305 E. Walnut Street, Des Moines, IA 50319, 1-515-281-5926, www.iowaattorneygeneral.gov.



Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. See **Section 6** for information on how to place a security freeze on your credit report.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting and Identity Security Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting and Identity Security Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting and Identity Security Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting and Identity Security Act. You can review your rights pursuant to the Fair Credit Reporting and Identity Security Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-877-566-7226 (toll free within North Carolina) or 601-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. There were 133 Rhode Island residents impacted by the incident. Under Rhode Island law, you have the right to obtain any police report filed in regard to the incident.

All U.S. Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

<<Company Logo>>

P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<Enrollment Code>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

July 28, 2023

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of an incident that may have affected your personal information and are providing you with information on additional steps you can consider taking to protect your personal information.

You are receiving this notice because you are an employee, former employee, job applicant, or spouse, dependent, or beneficiary of an employee or former employee of Group 1001 Resources, LLC, G1001 Advisory Resources, LLC, or their predecessor companies.

What Happened

On February 9, 2023, we were alerted to the existence of sophisticated ransomware on our information technology infrastructure. We immediately took steps to isolate and secure our systems and investigate the incident. We retained a leading third-party forensics firm to conduct a thorough investigation, secure our systems, remediate any risks, and methodically bring our systems back online once such systems were validated as clean. We also alerted appropriate regulatory authorities and the Federal Bureau of Investigation.

As part of our investigation, we determined that an unauthorized malicious actor accessed and acquired certain files from our systems. We have been analyzing the impacted files to understand what personal information may be at risk. The process of locating personal information in the acquired files and matching that information to individuals was complex. This work was substantially completed on July 10, 2023. We then began notifying the individuals whose personal information is confirmed to have been included, including you.

What Information Was Involved

The type of personal information at risk differs from individual to individual but may have included the following information relating to you: name, address, date of birth, Social Security number, driver's license or passport number, insurance, and other benefits information, such as the names of your dependents and beneficiaries.

What We Are Doing

Together with our forensics experts, our team scanned our systems for, and remediated, any identified indicators of compromise. Out of an abundance of caution, we have deployed additional advanced endpoint detection and monitoring tools on our newly restored systems for an added layer of security and visibility across our network. We will also continue to make infrastructure enhancements to strengthen and harden the security posture of our network and systems in the days, months, and years ahead.

Exhibit E

In addition, we are offering you identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. The IDX identity protection package includes: Experian, Equifax, and TransUnion credit monitoring, CyberScan™ dark web monitoring, identity theft insurance (for up to \$1,000,000 with no deductible), and fully managed identity restoration services. In some states, these services are required by law. We are offering these services to all affected individuals free of charge for 24 months, regardless of their state of residence.

What You Can Do

We encourage you to enroll and contact IDX with any questions. To enroll in the free identity protection services, please scan the QR code on the first page, or call 1-888-331-6462 or go to <https://app.idx.us/account-creation/protect> and use the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is October 28, 2023.

Once you enroll in these identity protection services, IDX will help you resolve issues if you determine your identity is compromised. To receive the credit monitoring services, you must be over the age of 18, have established credit in the United States, have a Social Security number in your name, and have a U.S. residential address associated with your credit file. If you do not have a credit file or are under the age of 18, you will not be able to register for the credit monitoring services, but you will receive CyberScan™ dark web monitoring, identity theft insurance, and the fully managed identity restoration services from IDX.

Although we have not received any reports of misuse of your information, it is always a good practice to be vigilant and closely review and monitor your financial accounts, statements, credit reports, and other financial information for any evidence of unusual activity, fraudulent charges, or signs of identity theft.

IDX representatives have been fully informed regarding the incident and are ready to answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed “Additional Steps You Can Take” document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-888-331-6462 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,



Victoria R. Lindamood
Chief Human Resources Officer

(Enclosure)



Additional Steps You Can Take

- 1. Website and Enrollment.** Scan the QR code or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your unique Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
- 3. Telephone.** Contact IDX at 1-888-331-6462 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
- 4. Review your credit reports.** It is always advisable to remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify IDX immediately by calling or by logging into the IDX website and filing a request for help. If you file a request for help or report suspicious activity, you will be contacted by a member of IDX's ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, IDX will assign you an ID Care Specialist who will work on your behalf.

You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General of your state.

5. Place Fraud Alerts with any of the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will

need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer credit reporting agencies by regular, certified, or overnight mail at the addresses below or, if available, comply with the consumer credit reporting agencies' online security freeze request procedures:

Equifax Security Freeze
1-888-298-0045
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion Security Freeze
1-888-909-8872
www.transunion.com
P.O. Box 160
Woodlyn, PA 19094

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past 5 years, provide the addresses where you have lived over the prior 5 years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have 3 business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to you within 5 days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual to access your credit report, you must call or send a written request to the credit reporting agencies by mail, or, if available, comply with the credit reporting agencies' online procedures for lifting a security freeze and provide proper identification (name, address, and Social Security number), and the PIN or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report, or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receipt of your request to lift the security freeze as requested.

To remove the security freeze, you must send a written request to each of the credit reporting agencies by mail or, if available, comply with the credit reporting agencies' online procedures for removing a security freeze. The credit reporting agencies have 3 business days after receipt of your request to remove the security freeze.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The **Federal Trade Commission** also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's office to report suspected incidents of identity theft at Iowa Attorney General's Office, Director of Consumer Protection Division, 1305 E. Walnut Street, Des Moines, IA 50319, 1-515-281-5926, www.iowaattorneygeneral.gov.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. Massachusetts law also allows consumers to place a security freeze on their credit reports. See **Section 6** for information on how to place a security freeze on your credit report.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting and Identity Security Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting and Identity Security Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting and Identity Security Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting and Identity Security Act. You can review your rights pursuant to the Fair Credit Reporting and Identity Security Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-877-566-7226 (toll free within North Carolina) or 601-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. There were <<RI Variable Count>> Rhode Island residents impacted by the incident. Under Rhode Island law, you have the right to obtain any police report filed in regard to the incident.

All U.S. Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.


[Login](#)


Privacy Policy

Effective Date: January 1, 2021

This Privacy Notice ("Notice") describes our practices for collecting, using and disclosing information that Clear Spring Life and Annuity Company ("Clear Spring Life," "we," "us," or "our") and our affiliates, including Clear Spring Life Marketing, LLC ("CSL Marketing"), may collect about you. This Notice applies to information we collect via Clear Spring Life websites or online services that display or link to this Notice (the "Services"). This Notice also applies to communications you may have with us

1. PERSONAL INFORMATION WE COLLECT

a. Personal Information We Collect Directly from You

We collect personal information from you when you use our Services and interact with us. The information we collect includes: any information you choose to provide us, such as first and last name, account name, address, Social Security number, contact information (e.g., telephone number) and any interest you may express in our products and services. In some circumstances, we may be required to collect information such as government-issued ID and proof of address. We may also collect information relating to:

- Records and copies of your correspondence (including email addresses and audio recordings of calls placed to our customer service representatives), if you contact us.
- Your responses to surveys, such as those that we might ask you to complete for research purposes.
- Details of potential transactions or transactions you carry out through us or financial products and services you purchase, including financial information.

b. Personal Information We Collect Automatically

We collect information automatically when you interact with our Services online. For example, we use cookies and other similar technologies to collect information about you as you use our Services. Examples of this type of information include the dates and times of your use of the Services, your IP (Internet Protocol) address, your browser type, your operating system, device identifiers, search history and the webpages or content to or from which you navigate.

Third parties may use cookies or similar technologies on our Services. For example, these technologies may be used to provide content, advertisements, and other services. We do not control third parties who may use these technologies to collect personal information about you, including information about your online activities over time and across different web sites when you use our Services.

c. Personal Information We Collect from Third Parties

We also collect information about you from third parties, which may include information from analytics and information providers. We may combine information we collect about you with information from third parties.

2. HOW WE USE YOUR INFORMATION

We use the information we gather to provide services to you, to respond to your inquiries, and for our business purposes. This includes:

- Authenticating your identity and/or your access to an account;

Exhibit F

- Initiating, facilitating, processing, and/or executing transactions;
- Responding to your requests and questions;
- Communicating with you regarding your account or any Services you use;
- Performing creditworthiness, fraud prevention or other similar reviews;
- Evaluating applications;
- Comparing information for accuracy and verification purposes;
- Managing our business and protecting ourselves, you, other persons, and the Services;
- Providing a personalized experience and implementing your preferences;
- Better understanding our customers and how they use and interact with the Services;
- Complying with our policies and obligations, government orders, legal advice or legal process;
- Establishing, exercising or defending our legal rights where it is necessary for our legitimate interests or the legitimate interests of others;
- Resolving disputes, collecting fees, or troubleshooting problems; and
- Providing customer service to you or otherwise communicating with you.

We may also process your personal information to fulfill the purposes for which you provide it, or with your consent.

3. HOW WE SHARE INFORMATION

We may disclose the information we gather with our affiliates and third parties. For example, we may share information with:

- **Service providers and/or data processors:** We may share personal information with third-party service providers that perform services and functions at our direction and on our behalf. These third-party service providers may, for example, provide you with Services, verify your identity, assist in processing transactions, or provide customer support.
- **Other parties to transactions:** We may share information with the other participants to your transactions. This may include: nonaffiliated third parties who are assisting us by performing services or functions for us or on our behalf, such as agents, brokers, brokerage firms, and insurance agencies; and with your designee, including for the purpose of providing information regarding the status of a transaction.
- **Other third parties:**
 - To comply with any legal, regulatory or contractual obligation, or with any legal or regulatory process (such as a valid court order or subpoena) or advice of counsel;
 - To third parties to market our products or services to you, or to track the effectiveness of such marketing, including banks, insurance agencies and securities brokers or dealers, with whom we have written distribution or joint marketing agreements;
 - To establish, exercise, or defend legal claims or our policies;
 - If we believe disclosure is necessary or appropriate to protect the rights, property, or safety of ourselves, our customers, or others. This includes exchanging information with other companies and organizations for the purposes of fraud prevention and credit risk reduction;
 - In connection with the purchase, sale, merger, consolidation or transfer of all or part of our business; or
 - We may also use the information we collect for our own or our service providers' other operational purposes, purposes for which we provide you additional notice, or for purposes compatible with the context in which the personal information was collected.

We may also disclose data to fulfill the purposes for which you provide it, or with your consent.

4. YOUR CHOICES

If we engage in email marketing, we will provide you the option to opt out of such communications, as required by law. As of the Effective Date listed above, there is no commonly accepted response for Do Not Track signals initiated by browsers. Therefore, we do not respond to such signals or to other mechanisms that provide the ability to exercise choice regarding the collection of personally identifiable information regarding your online activities over time and across third-party web sites or online services.

You can control the use of cookies with respect to the individual browser(s) you use to access our Services. If you reject cookies, you may still use our website, but your ability to use some features or areas of our website may be limited. You may control how your browser accepts cookies; please see your browser help documentation.

5. SECURITY

We have implemented administrative, physical and technical safeguards designed to protect your personal information. However, we cannot guarantee the security or confidentiality of information you transmit to us or receive from us when using the Services.

6. PRIVACY NOTICE FOR CALIFORNIA RESIDENTS

(Effective July 1, 2023)

The California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act (collectively, the "CCPA") gives California residents certain privacy rights with respect to some of the personal information Clear Spring Life and Annuity Company ("Clear Spring Life," "we," "us" or "our") may collect about you. We have adopted this California Privacy Notice ("Privacy Notice") in accordance with the notice requirements under the CCPA. Any terms defined in the CCPA have the same meaning when used in this Privacy Notice. This Privacy Notice does not apply to information we collect pursuant to the Gramm-Leach-Bliley Act.

This Privacy Notice applies only to information collected through the following websites we own: <https://www.clearspringlife.com>.

Definitions Specific to this Privacy Notice

The CCPA includes definitions for terms specific to this Privacy Notice that do not apply to our primary Notice, including the following terms:

"Personal Information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal Information does not include publicly available information obtained from government records; deidentified or aggregated consumer information that cannot be reconstructed to identify you; any information covered under the Gramm-Leach-Bliley Act or the California Financial Information Privacy Act, activities covered by the Fair Credit Reporting Act, or protected health information as defined under the Health Insurance Portability and Accountability Act. Personal Information also includes "Sensitive Personal Information," as defined below, except where otherwise noted.

"Sale" or "sell" means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a Third Party for monetary or other valuable consideration.

"Share" or "sharing" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's Personal Information by the business to a Third Party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a Third Party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged.

"Sensitive Personal Information" means Personal Information that reveals a consumer's Social Security number, driver's license, state identification card, or passport number; account log-in, financial account number, debit card number, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; precise geolocation; racial or ethnic origin, religious beliefs, or union membership; contents of email or text messages; and genetic data. Sensitive Personal Information also includes Processing of biometric information for the purpose of uniquely identifying a consumer and Personal Information collected and analyzed concerning a consumer's health, sex life, or sexual orientation.

"Service Provider" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's Personal Information for a business purpose pursuant to a written contract.

"Third Party" means a person or entity who is not any of the following:

1. The business with whom the consumer intentionally interacts and that collects personal information from the consumer as part of the consumer's current interaction with the business under this title.
2. A Service Provider to the business.
3. A Contractor.

"Vendor" means a Service Provider, contractor, or processor as those terms are defined in the CCPA.

To the extent other terms used in this Privacy Notice are defined terms under the CCPA, they shall have the meanings afforded

to them in that statute, whether or not capitalized, herein.

Collection and Processing of Personal Information

We, and our Vendors, collect the following categories of Personal Information about our consumers. The categories of Personal Information we collect about a specific consumer will depend on our relationship or interactions with such consumer. We also have collected or Processed the following categories of Personal Information about consumers in the preceding 12 months:

1. Identifiers, such as name, alias, online identifiers, account name, physical characteristics or description;
2. Contact and financial information, including phone number, address, email address, financial information, medical information, health insurance information;
3. Characteristics of protected classifications under state or federal law, such as age, gender, race, physical or mental health conditions, and marital status;
4. Biometric information (such as your fingerprint and photos for facial recognition or your voiceprint);
5. Commercial information, such as transaction information and purchase history;
6. Internet or other electronic network activity information, such as browsing history and interactions with our websites or advertisements;
7. Geolocation;
8. Audio, electronic, visual and similar information, such as call and video recordings;
9. Professional or employment-related information, such as work history and prior employer;
10. Education information, as defined in the federal Family Educational Rights and Privacy Act, such as student records and directory information; and
11. Inferences drawn from any of the Personal Information listed above to create a profile or summary about, for example, an individual's preferences and characteristics.

Data Retention

We retain Personal Information no longer than necessary to fulfill the purposes described in this Privacy Notice, and to comply with applicable laws and regulations. We consider the following criteria when determining how long to retain Personal Information: why we collected the Personal Information; the nature of the Personal Information; the sensitivity of the Personal Information; our legal obligations related to the Personal Information; and the risks associated with retaining the Personal Information.

Purposes for Processing Personal Information

The purposes for which we collect, Process or disclose Personal Information is based on our relationship with you and the interactions you have with us. We, and our Vendors, collect, Process, or disclose Personal Information (excluding Sensitive Personal Information) to:

- Operate, manage, and maintain our business;
- Provide, develop, improve, repair, and maintain our products and services;
- Personalize, advertise, and market our products and services;
- Conduct research, analytics, and data analysis;
- Maintain our facilities and infrastructure;
- Undertake quality and safety assurance measures;
- Conduct risk and security controls and monitoring;
- Detect and prevent fraud;
- Perform identity verification;
- Perform accounting, audit, and other internal functions, such as internal investigations;
- Comply with law, legal process, and internal policies;
- Receive and respond to inquiries;
- Maintain records;
- Exercise and defend legal claims; and
- Otherwise accomplish our business purposes and objectives.

We, and our Vendors, do not collect or Process Sensitive Personal Information.

We do not sell or share and have not sold or shared Personal Information about California consumers in the past twelve months. Relatedly, we do not have actual knowledge that we sell or share Personal Information of California consumers who

are under 16 years of age.

Categories of Personal Information We Disclose to Vendors & Third Parties

1. Identifiers, such as name, alias, online identifiers, account name, physical characteristics or description;
2. Contact and financial information, including phone number, address, email address, financial information, medical information, health insurance information;
3. Characteristics of protected classifications under state or federal law, such as age, gender, race, physical or mental health conditions, and marital status;
4. Biometric information (such as your fingerprint and photos for facial recognition or your voiceprint);
5. Commercial information, such as transaction information and purchase history;
6. Internet or other electronic network activity information, such as browsing history and interactions with our websites or advertisements;
7. Geolocation;
8. Audio, electronic, visual and similar information, such as call and video recordings;
9. Professional or employment-related information, such as work history and prior employer;
10. Education information, as defined in the federal Family Educational Rights and Privacy Act, such as student records and directory information; and
11. Inferences drawn from any of the Personal Information listed above to create a profile or summary about, for example, an individual's preferences and characteristics.

Sources from Which We Collect Personal Information

We collect Personal Information directly from consumers, as well as from joint marketing partners, public databases, providers of demographic data, publications, professional organizations, social media platforms, and Vendors and Third Parties when they disclose Personal Information to us based on your interactions with them.

Categories of Entities to Whom We Disclose Personal Information

- **Affiliates & Vendors.** We disclose the categories of Personal Information listed in this Privacy Notice to our affiliates and Vendors for the purposes described in this Privacy Notice. Our Vendors provide us with services for our websites, as well as other products and services, such as web hosting, data analysis, payment processing, order fulfillment, customer service, infrastructure provision, technology services, email delivery services, credit card processing, legal services, and other similar services. We grant our Vendors access to Personal Information only to the extent needed for them to perform their functions, and we require them to protect the confidentiality and security of such information.
- **Third Parties.** We may also disclose the categories of Personal Information listed in this Privacy Notice to the following categories of Third Parties:
 - **At Your Direction.** We may disclose your Personal Information to any Third Party with your consent or at your direction.
 - **Business Transfers or Assignments.** We may disclose your Personal Information to other entities as reasonably necessary to facilitate a merger, sale, joint venture or collaboration, assignment, transfer, or other disposition of all or any portion of our business, assets, or stock (including in connection with any bankruptcy or similar proceedings).
 - **Legal and Regulatory.** We may disclose your Personal Information to government authorities, including regulatory agencies and courts, as reasonably necessary for our business operational purposes, to assert and defend legal claims, and otherwise as permitted or required by law.

California Resident Data Rights Requests

Consumers who live in California have certain rights with respect to the collection and use of their Personal Information. You may access these data rights by calling (800) 990-7626, by emailing us at compliance@clearspringlife.com or by [clicking here](#) and submitting details regarding your request.

Verification

We may ask you to provide information that will enable us to verify your identity in order to comply with your request. Further, when a consumer authorizes an agent to make a request on their behalf, we may require the agent to provide proof of signed permission from the consumer to submit the request, or we may require the consumer to verify their own identity to us or confirm with us that they provided the agent with permission to submit the request. Please note that there are circumstances in which we may not be able to comply with your request pursuant to the CCPA, including when we cannot verify your request

and/or when there is a conflict with our own obligations to comply with other legal or regulatory requirements. Additionally, in certain instances, some information we collect from you may be excluded from the definition of Personal Information as defined under the CCPA, as it is protected by the Gramm-Leach-Bliley Act, and as such, this information is exempt from certain rights otherwise available to you under the CCPA. We will respond to your request consistent with applicable law.

Data Rights

You have the following rights regarding our collection and use of your Personal Information, subject to certain exceptions.

1. **Right to Receive Information on Privacy Practices:** you have the right to receive the following information at or before the point of collection:
 - a. The categories of Personal Information to be collected;
 - b. The purposes for which the categories of Personal Information are collected or used;
 - c. Whether or not that Personal Information is sold or shared;
 - d. If the business collects Sensitive Personal Information, the categories of Sensitive Personal Information to be collected, the purposes for which it is collected or used, and whether that information is sold or shared; and
 - e. The length of time the business intends to retain each category of Personal Information, or if that is not possible, the criteria used to determine that period.

We have provided this information in this Privacy Notice, and you may request further information about our privacy practices by contacting us at the contact information provided in this Privacy Notice.

2. **Right to Deletion:** You may request that we delete any Personal Information about you we that we collected from you.
3. **Right to Correction:** You may request that we correct any inaccurate Personal Information we maintain about you.
4. **Right to Know:** You may request that we provide you with information about what Personal Information we have collected about you, including:
 - a. The categories of Personal Information we have collected about you;
 - b. The categories of sources from which we collected such Personal Information;
 - c. The business or commercial purpose for collecting, selling, or sharing Personal Information about you;
 - d. The categories of Third Parties to whom we disclose such Personal Information; and
 - e. The specific pieces of Personal Information we have collected about you.
5. **Right to Receive Information About Onward Disclosures:** You may request that we disclose to you:
 - a. The categories of Personal Information that we have collected about you;
 - b. The categories of Personal Information that we have sold or shared about you and the categories of Third Parties to whom the Personal Information was sold or shared; and
 - c. The categories of Personal Information we have disclosed about you for a business purpose and the categories of persons to whom it was disclosed for a business purpose.
6. **Right to Non-Discrimination:** You have the right not to be discriminated against for exercising your data rights. We will not discriminate against you for exercising your data rights.

Sale and Sharing of Your Personal Information and Use of Your Sensitive Personal Information: We do not sell or share and have not sold or shared Personal Information of California consumers in the past twelve months. Further, we do not use Sensitive Personal Information for purposes beyond those authorized by the CCPA, and we have not used Sensitive Personal Information of California consumers in the preceding twelve months for purposes beyond those authorized by the CCPA. Because we do not sell or share Personal Information or use or disclose Sensitive Personal Information for purposes other than those authorized by the CCPA, we do not process opt-out preference signals of California consumers. If we ever do sell or share Personal Information of California consumers or use Sensitive Personal Information for purposes beyond those authorized by the CCPA, we will provide you with the right to opt-out of the sale and sharing of your Personal Information or limit the use of your Sensitive Personal Information to the purposes authorized by the CCPA, as applicable.

California Residents Under 18. If you are a resident of California under the age of 18 and a registered user of our website, you may ask us to remove content or data that you have posted to the website by writing to compliance@clearspringlife.com. Please note that your request does not ensure complete or comprehensive removal of the content or data as, for example, some of your content or data may have been reposted by another user.

Disclosure About Direct Marketing. California Civil Code § 1798.83 permits California residents to annually request certain information regarding our disclosure of Personal Information to other entities for their direct marketing purposes in the preceding calendar year. We do not distribute your Personal Information to other entities for their own direct marketing purposes.

Financial Incentives for California Consumers. We do not provide financial incentives to California consumers who allow us to collect, retain, sell, or share their Personal Information. We will describe such programs to you if and when we offer them to you.

Changes to our Supplemental Notice. We reserve the right to amend this Privacy Notice in our discretion and at any time. When we make material changes to this Privacy Notice, we will notify you by posting an updated Privacy Notice on our website and listing the effective date of such updates.

Contacting Us. If you have any questions, comments, requests, or concerns related to this Privacy Notice, Clear Spring Life's information practices, or how to access this Privacy Notice in another format, please contact us by mail at 10555 Group 1001 Way, Zionsville, IN 46077, by email at compliance@clearspringlife.com, or by calling (800) 990-7626.

7. CHANGES TO THIS PRIVACY NOTICE

We reserve the right to modify this Notice from time to time, and, we will notify you of changes to this Notice by revising this Notice and updating the Effective Date above.

8. CONTACT US

We take your privacy concerns seriously. If you have any questions about this Notice or if you believe that we have not complied with this Notice with respect to your personal information, you may call us at (800)990-7626 or write to compliance@clearspringlife.com.

About Us

Our commitment is to advance the strategic interests of our clients and to deliver long-term results with excellence and integrity.

Our Company

[Privacy and Security Policy](#)
[Terms and Conditions](#)

Initiatives

[Indy Women in Tech](#)

Contact Us

Clear Spring Life and Annuity Company
PO Box 80509
Indianapolis, IN 46280
marketing@cslmarketing.com



Privacy Policy

Introduction

At Delaware Life, protecting your privacy is important to us. Whether you are an existing customer or considering a relationship with us, we recognize that you have an interest in how we may collect, use and share information about you.

We understand and appreciate the trust and confidence you place in us, and we take seriously our obligation to maintain the confidentiality and security of your personal information.

We invite you to review this Privacy Policy which outlines how we use and protect that information.

Collection of Nonpublic Personal Information by Delaware Life

Collecting personal information from you is essential to our ability to offer you high-quality investment, retirement and insurance products. When you apply for a product or service from us, we need to obtain information from you to determine whether we can provide it to you. As part of that process, we may collect information about you, known as nonpublic personal information, from the following sources:

- Information we receive from you on applications or other forms, such as your name, address, social security number and date of birth;
- Information about your transactions with us, our affiliates or others, such as other life insurance policies or annuities that you may own; and
- Information we receive from a consumer reporting agency, such as a credit report.

Limited Use and Sharing of Nonpublic Personal Information by Delaware Life

We use the nonpublic personal information we collect to help us provide the products and services you have requested and to maintain and service your accounts. Once we obtain nonpublic personal information from you, we do not disclose it to any third party except as permitted or required by law.

We may share your nonpublic personal information within Delaware Life to help us develop innovative financial products and services. Delaware Life provides a wide variety of financial products and services including individual life insurance, and individual fixed and variable annuities.

We also may disclose your nonpublic personal information to companies that help in conducting our business or perform services on our behalf. Delaware Life is highly selective in choosing these companies, and we require them to comply with strict standards regarding the security and confidentiality of our customers' nonpublic personal information. These companies may use and disclose the information provided to them only for the purpose for which it is provided, as permitted by law.

There also may be times when Delaware Life is required to disclose its customers' nonpublic personal information, such as when complying with federal, state or local laws, when responding to a subpoena, or when complying with an inquiry by a governmental agency or regulator.

Companies that share your information with third parties for marketing purposes must offer their customers an opt-out program. Because we do not share your information with third parties for such purposes or for any reason not allowed by law, an opt-out program is not needed nor required.

Exhibit G

Our Treatment of Information about Former Customers

Our protection of your nonpublic personal information extends beyond the period of your customer relationship with us. If your customer relationship with us ends, we will not disclose your information to non-affiliated third parties other than as permitted or required by law.

Security of Your Nonpublic Personal Information

We maintain physical, electronic and procedural safeguards that comply with federal and state regulations to safeguard your nonpublic personal information from unauthorized use or improper access.

Employee Access to Your Nonpublic Personal Information

We restrict access to your nonpublic personal information to those employees who have a business need to know that information in order to provide products or services to you or to maintain your accounts. Our employees are governed by a strict code of conduct and are required to maintain the confidentiality of customer information.

Questions

If you have questions about our privacy practices and policy please contact the Privacy Officer at Privacy@delawarelife.com. All concerns will be handled discreetly and confidentially.

delawarelife.com

Delaware Life Insurance Company (Waltham, MA) is authorized to transact business in all states (except New York), the District of Columbia, Puerto Rico and the U.S. Virgin Islands. Delaware Life Insurance Company of New York is authorized to transact business in New York and Rhode Island. Both companies are members of Group One Thousand One, LLC ("Group1001"). Each company is responsible for its own financial condition and contractual obligations.

© 2019 Delaware Life Insurance Company. All rights reserved.

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS

Cary Weigand, Cheryl Schmidt, and Calvin Schmidt, et al.

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

(c) Attorneys (Firm Name, Address, and Telephone Number)

Lynn A. Toops, Cohen and Malad, LLP
One Indiana Square, Suite 1400, Indianapolis, IN 46204

DEFENDANTS

Group 1001 Insurance Holdings, LLC; Clear Spring Life and Annuity Company; Delaware Life Ins. Company

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

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

Attorneys (If Known)

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

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

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

Table with columns for Plaintiff (PTF) and Defendant (DEF) citizenship: Citizen of This State, Citizen of Another State, Citizen or Subject of a Foreign Country, Incorporated or Principal Place of Business In This State, Incorporated and Principal Place of Business In Another State, Foreign Nation.

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

Click here for: Nature of Suit Code Descriptions.

Large table with categories: CONTRACT, REAL PROPERTY, CIVIL RIGHTS, TORTS, PRISONER PETITIONS, HABES CORPUS, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES.

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

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

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity): 28 U.S.C. Section 1332 (d)
Brief description of cause: Class action lawsuit for damages and other relief arising from unauthorized disclosure of personal information in data breach.

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P. DEMAND \$ CHECK YES only if demanded in complaint: JURY DEMAND: Yes No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE DOCKET NUMBER

DATE SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

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

- I.(a) Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
- (b) County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)
- (c) Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".
- II. Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here. United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: [Nature of Suit Code Descriptions](#).
- V. Origin.** Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.
- VII. Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

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

Civil Action No. _____

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____
was received by me on *(date)* _____ .

I personally served the summons on the individual at *(place)* _____
_____ on *(date)* _____ ; or

I left the summons at the individual's residence or usual place of abode with *(name)* _____
_____, a person of suitable age and discretion who resides there,
on *(date)* _____ , and mailed a copy to the individual's last known address; or

I served the summons on *(name of individual)* _____ , who is
designated by law to accept service of process on behalf of *(name of organization)* _____
_____ on *(date)* _____ ; or

I returned the summons unexecuted because _____ ; or

Other *(specify)*: _____ .

My fees are \$ _____ for travel and \$ _____ for services, for a total of \$ _____ .

I declare under penalty of perjury that this information is true.

Date: _____

Server's signature

Printed name and title

Server's address

Additional information regarding attempted service, etc:

AO 440 (Rev. 06/12) Summons in a Civil Action (Page 2)

Civil Action No. _____

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____
was received by me on *(date)* _____.

I personally served the summons on the individual at *(place)* _____
_____ on *(date)* _____; or

I left the summons at the individual's residence or usual place of abode with *(name)* _____
_____, a person of suitable age and discretion who resides there,
on *(date)* _____, and mailed a copy to the individual's last known address; or

I served the summons on *(name of individual)* _____, who is
designated by law to accept service of process on behalf of *(name of organization)* _____
_____ on *(date)* _____; or

I returned the summons unexecuted because _____; or

Other *(specify)*: _____.

My fees are \$ _____ for travel and \$ _____ for services, for a total of \$ _____.

I declare under penalty of perjury that this information is true.

Date: _____

Server's signature

Printed name and title

Server's address

Additional information regarding attempted service, etc:

AO 440 (Rev. 06/12) Summons in a Civil Action (Page 2)

Civil Action No. _____

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____
was received by me on *(date)* _____ .

I personally served the summons on the individual at *(place)* _____
_____ on *(date)* _____ ; or

I left the summons at the individual's residence or usual place of abode with *(name)* _____
_____, a person of suitable age and discretion who resides there,
on *(date)* _____ , and mailed a copy to the individual's last known address; or

I served the summons on *(name of individual)* _____ , who is
designated by law to accept service of process on behalf of *(name of organization)* _____
_____ on *(date)* _____ ; or

I returned the summons unexecuted because _____ ; or

Other *(specify)*: _____ .

My fees are \$ _____ for travel and \$ _____ for services, for a total of \$ _____ .

I declare under penalty of perjury that this information is true.

Date: _____

Server's signature

Printed name and title

Server's address

Additional information regarding attempted service, etc:

AO 440 (Rev. 06/12) Summons in a Civil Action (Page 2)

Civil Action No. _____

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____
was received by me on *(date)* _____.

I personally served the summons on the individual at *(place)* _____
_____ on *(date)* _____; or

I left the summons at the individual's residence or usual place of abode with *(name)* _____
_____, a person of suitable age and discretion who resides there,
on *(date)* _____, and mailed a copy to the individual's last known address; or

I served the summons on *(name of individual)* _____, who is
designated by law to accept service of process on behalf of *(name of organization)* _____
_____ on *(date)* _____; or

I returned the summons unexecuted because _____; or

Other *(specify)*: _____.

My fees are \$ _____ for travel and \$ _____ for services, for a total of \$ _____.

I declare under penalty of perjury that this information is true.

Date: _____

Server's signature

Printed name and title

Server's address

Additional information regarding attempted service, etc: