Exhibit A

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

LAMONT BRACY, *on behalf of himself and all others similarly situated,*	)	
Plaintiff,	)	Case No. _____
v.	)	
AMERICOLD LOGISTICS LLC,	)	
Defendant.	)	**JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Lamont Bracy ("Plaintiff") brings this Class Action Complaint against Americold Logistics LLC ("Defendant" or "Americold"), on behalf of himself and all others similarly situated ("Class Members"), and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information and protected health information (collectively "PII") including, but not limited to full names, Social Security numbers, addresses, driver's license numbers, state identification

numbers, passport numbers, financial account information, health insurance information, and medical information.

2. Defendant is an international warehousing and logistics company headquartered in Atlanta, Georgia.

3. In the ordinary course of Defendant's business, Defendant acquires, possesses, analyzes, and otherwise utilizes Plaintiff's and putative Class Members' PII.

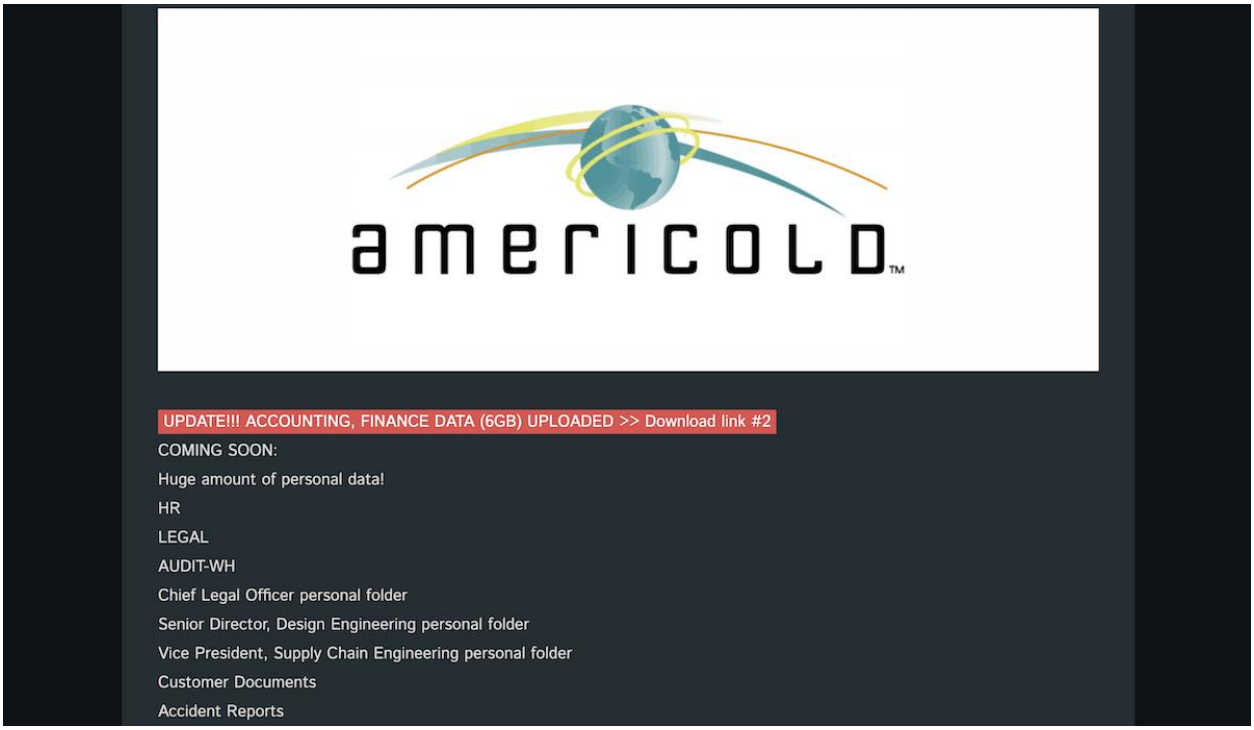
4. With this action, Plaintiff seeks to hold Defendant responsible for the harms it caused and will continue to cause Plaintiff and at least 129,611 other similarly situated persons[1] in the massive and preventable cyberattack purportedly discovered by Defendant on or around April 26, 2023, by which cybercriminals infiltrated Defendant's inadequately protected network servers and accessed and exfiltrated highly sensitive PII belonging to Plaintiff and Class Members which was being kept unprotected (the "Data Breach").

5. The Cactus cybercriminal ransomware gang claimed that it accessed and exfiltrated Plaintiff's and Class Members' PII.[2]

---

[1] Data Breach Notifications, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/80071f08-cdaa-4ca5-8efb-a2bf28c33fe5.shtml (last visited December 13, 2023).

[2] https://www.bleepingcomputer.com/news/security/cold-storage-giant-americold-discloses-data-breach-after-april-malware-attack/ (last visited December 13, 2023).



6. The Cactus gang leaked a 6 gigabyte archive of accounting and financial documents they allegedly stole from Americold's network, including sensitive private information.[3]

7. Plaintiff further seeks to hold Defendant responsible for not ensuring that Defendant maintained the PII in a manner consistent with industry standards.

8. On or about December 8, 2023, Defendant notified state Attorneys General and many Class Members about the widespread Data Breach (the "Notice Letter").[4]

[3] *Id.*

[4] Sample Notice Letter available at the Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/80071f08-cdaa-4ca5-8efb-a2bf28c33fe5/640792d8-8dc2-4b9c-9f0a-ebcd6ee14b4e/document.html (last

9. Despite knowing that PII stolen in the Data Breach would be used for harm, Defendant did not begin notifying victims, like Plaintiff, or state Attorneys General of the Data Breach until December 8, 2023, over 7 months later -- long after Defendant understood the risk that Plaintiff and Class Members faced. And when the Notice Letters were finally sent, Defendant omitted crucial information, such as the fact that the Data Breach was a ransomware attack by a known criminal hacker group, and as a result, Plaintiff's and Class Members' PII was likely disseminated on the Dark Web. As a result of this delayed response, Plaintiff and Class Members were unaware that their Private Information had been compromised, and that Plaintiff and Class Members were, and continue to be, at a present and significant risk of identity theft and various other forms of personal, social, and financial harm.

10. The Notice Letter provides no further information regarding the Data Breach and only recommends how victims can place a fraud alert or credit freeze on their account and how to sign up for the limited identity monitoring services Defendant offered in response to the Data Breach. The Notice Letter does not explain how the Data Breach occurred, what steps Defendant took following the Data Breach, whether Defendant made any changes to its data security, or most importantly, whether Plaintiff's and Class Members' PII remains in the possession of criminals.

---

visited Dec. 13, 2023).

11. By acquiring, utilizing, and benefiting from Plaintiff's and Class Members' PII for its business and employment purposes, Defendant owed or otherwise assumed common law, contractual, and statutory duties that extended to Plaintiff and Class Members. These duties required Defendant to design and implement adequate data security systems to protect Plaintiff's and Class Members' PII in its possession and to keep Plaintiff's and Class Members' PII confidential, safe, secure, and protected from unauthorized disclosure, access, dissemination, or theft.

12. Defendant breached these duties by failing to implement adequate data security measures and protocols to properly safeguard and protect Plaintiff's and Class Members' PII from a foreseeable cyberattack on its systems that resulted in the unauthorized access and theft of Plaintiff's and Class Members' PII.

13. Currently, the full extent of the types of PII, the scope of the breach, and the root cause of the Data Breach are all within the exclusive control of Defendant, its agents, counsel, and forensic security vendors at this phase of the litigation.

14. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized

disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the Plaintiff's and Class Members' PII was compromised through disclosure to an unknown and unauthorized criminal third party.

15. Upon information and belief, Defendant breached its duties and obligations in one or more of the following ways: (1) failing to design, implement, monitor, and maintain reasonable network safeguards against foreseeable threats; (2) failing to design, implement, and maintain reasonable data retention policies; (3) failing to adequately train staff on data security; (4) failing to comply with industry-standard data security practices; (5) failing to warn Plaintiff and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately encrypt the PII; (7) failing to recognize or detect that its network had been compromised and accessed in a timely manner to mitigate the harm; (8) failing to utilize widely available software able to detect and prevent this type of attack; and (9) otherwise failing to secure the hardware using reasonable and effective data security procedures free of foreseeable vulnerabilities and data security incidents.

16. Based on the type of sophisticated and targeted criminal activity, the type of PII involved, Defendant's admission that the PII was accessed, and the claims by a criminal ransomware that it was responsible for the Data Breach, it can be concluded that the unauthorized criminal third party was able to successfully target

Plaintiff's and Class Members' PII, infiltrate and gain access to Defendant's network, and exfiltrate Plaintiff's and Class Members' PII, including full names, Social Security numbers, addresses, driver's license numbers, state identification numbers, passport numbers, financial account information, health insurance information, and medical information, for the purposes of utilizing or selling the PII for use in future fraud and identity theft related cases.

17. As a result of Defendant's failures and the Data Breach, Plaintiff's and Class Members' identities are now at a current and substantial imminent and ongoing risk of identity theft and shall remain at risk for the rest of their lives.

18. As Defendant instructed, advised, and warned in its Notice Letter discussed below, Plaintiff and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiff and Class Members have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will include into the future: (a) reviewing financial statements; (b) changing passwords; and (c) signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against and mitigating against the imminent risk of identity theft.

19. Plaintiff and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) financial costs

incurred mitigating the materialized risk and imminent threat of identity theft; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (c) financial costs incurred due to actual identity theft; (d) loss of time incurred due to actual identity theft; (e) loss of time heeding Defendant's warnings and following its instructions in the Notice Letter; (g) deprivation of value of their PII; (h) invasions of their privacy; and (i) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fail to undertake appropriate and adequate measures to protect it.

20. Plaintiff brings this action on behalf of all persons whose PII was compromised due to Defendant's failure to adequately protect Plaintiff's and Class Members' PII. Accordingly, Plaintiff brings this action against Defendant seeking redress for It unlawful conduct and asserts claims on behalf of the Class for Negligence, Breach of Implied Contract, Unjust Enrichment, Invasion of Privacy, and Violation of O.C.G.A. § 13-6-11.

PARTIES

21. Plaintiff Lamont Bracy is an adult individual and, at all relevant times herein, a resident and citizen of the state of Alabama, residing in Montgomery, Alabama, in Montgomery County.

22. Defendant Americold Logistics LLC is a limited liability company organized and existing under the laws of the State of Delaware, with its principal place of business at 10 Glenlake Parkway NE, 600 South Tower, Atlanta, Georgia. Defendant Americold Logistics LLC is a resident and citizen of Georgia. Americold Logistics LLC may be served by service of process upon its registered agent for same, CT Corporation System, 289 S Culver St., Lawrenceville, GA 30046-4805.

23. Upon information and belief, Americold Logistics LLC has at least one member, Americold Realty Trust, Inc., that is a resident and citizen of Georgia, with its address at 10 Glenlake Parkway South Tower, Suite 600, Atlanta, Georgia 30328-7250. Americold Logistics LLC is a subsidiary of Americold Realty Trust, Inc.[5]

24. Other members of the Defendant LLC who are only known to Defendant and who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to reflect the true names and capacity of additional members of Defendant LLC if they exist when their identities become known.

JURISDICTION AND VENUE

25. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy

[5] https://www.sec.gov/Archives/edgar/data/1455863/000162828020002690/exhibit211q419.htm (last visited Dec. 13, 2023).

exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class, including Plaintiff Bracy, is a citizen of a state different from Defendant.

26. This Court has general personal jurisdiction over Defendant Americold because Defendant's principal place of business is in this District and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

27. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's principal place of business is in this District.

FACTUAL ALLEGATIONS

Background

28. Defendant Americold is a "global leader in temperature-controlled warehousing and logistics, with the largest network in the word."[6] Defendant's services include warehousing and distribution services including blast freezing, pick n pack, labeling/relabeling, repacking, kitting, staging, cross-dock, light assembly, and food processing.

[6] https://www.americold.com/wp-content/uploads/sites/2/2020/07/Americold-Privacy-Notice-Jan-29-2020-v0.12.pdf (last visited Dec. 13, 2023).

29. Defendant Americold owns and operates over 245 temperature-controlled warehouses, with more than 1 billion cubic feet of storage, in the United States, Australia, New Zealand, China, Argentina, and Canada.

30. To provide these services, and in the ordinary course of Defendant's business, Defendant acquires, possesses, analyzes, and otherwise utilizes Plaintiff's and putative Class Members' PII.

31. Defendant's Privacy Policy, posted on its website, states that Americold only discloses personal data to "legal and regulatory authorities; our external advisors; our Processors; any party as necessary in connection with legal proceedings; any party as necessary for investigating, detecting or preventing criminal offenses; any purchaser of our business; and any third party providers of advertising, plugins or content used on our Sites or our Apps."[7]

32. Defendant's Privacy Policy further state that it has "implemented appropriate technical and organizational security measures designed to protect your Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, unauthorized access, and other unlawful or unauthorized forms of Processing, in accordance with applicable law."[8]

---

[7] *Privacy Policy*, https://www.americold.com/wp-content/uploads/sites/2/2021/08/Americold-Privacy-Notice_21-08-05.pdf (last visited Dec 13, 2023).

[8] *Id.*

Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members

33. In the ordinary course of its business and for employment purposes, Americold maintains the PII of its customers, current and past employees, consumers, and others, including but not limited to: full names, Social Security numbers, addresses, driver's license numbers, state identification numbers, passport numbers, financial account information, health insurance information, and medical information.

34. Additionally, Defendant may receive PII from other individuals and/or organizations including Plaintiff's and Class Members' employers, insurance carriers, and in connection with enrollment in employee insurance and retirement benefit plans.

35. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to consumers and employees, Defendant, upon information and belief, promises to, among other things: keep protected health information private; comply with industry standards related to data security and PII, inform consumers of its legal duties and comply with all federal and state laws protecting consumer PII; only use and release PII for reasons that relate to medical care and treatment, and, provide adequate notice to individuals if their PII is disclosed without authorization.

36. At every step, Defendant acquires and maintains sensitive PII and has

a duty to protect that PII from unauthorized access.

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

38. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

39. Plaintiff and Class Members relied on Defendant to implement and follow adequate data security policies and protocols, to keep their PII confidential and securely maintained, to use their PII solely for proper business services and purposes, and to prevent the unauthorized disclosure of their PII.

The Cyberattack and Data Breach

40. Beginning on or around December 8, 2023, Defendant issued Notice Letters to Plaintiff and Class Members. In total, at least 129,611 individuals were impacted by the Data Breach.[9]

41. Americold informed Plaintiff and other Class Members that on April 26, 2023, Americold became aware of a cybersecurity incident that involved the

[9] See *Data Breach Notifications*, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/80071f08-cdaa-4ca5-8efb-a2bf28c33fe5.shtml (last visited Dec. 13, 2023).

deployment of malware on certain parts of its computer systems.[10]

42. Americold took steps to secure its network systems and investigated the nature and scope of the incident with the consultation of outside counsel and a leading third-party cybersecurity firm.[11]

43. Through its investigation, Americold determined that its network and servers were subject to a cyberattack that impacted its network resulting in information on its network being accessed and acquired without authorization.[12]

44. Plaintiff's and Class Members' PII was exfiltrated and stolen in the attack.

45. Furthermore, the investigation determined that the accessed systems contained PII. This PII was accessible, unencrypted, unprotected, and vulnerable to acquisition and/or exfiltration by the unauthorized actor.

46. The type of PII accessed by the unauthorized actor in the Data Breach includes full names, Social Security numbers, addresses, driver's license numbers, state identification numbers, passport numbers, financial account information, health insurance information, and medical information.[13]

---

[10] *See* Notice Letter

[11] *Id.*

[12] *Id.*

[13] *Id.*

47. While Americold stated in the Notice Letter that the unusual activity occurred and was discovered on April 26, 2023, Americold did not begin notifying victims until December 8, 2023 - over 7 months after Americold discovered the Data Breach occurred.[14]

48. Defendant had obligations created by contract, industry standards, common law, and its own promises and representations to keep Plaintiff's and Class Members' PII confidential and to protect it from unauthorized access and disclosure.

49. Plaintiff and Class Members provided their PII directly, or indirectly, to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

50. Through its Notice Letter, Americold also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to take steps to mitigate their risk of identity theft, such as reviewing financial accounts, and reviewing credit reports for possible fraud.

51. Americold advised breach victims to "remain vigilant over the next twelve to twenty-four months against potential identity theft and fraud by carefully reviewing credit reports and account statements to endure that all activity is valid."[15]

[14] *Id.*

[15] *Id.*

52. Americold has offered abbreviated, non-automatic credit monitoring services to victims thereby identifying the harm posed to Plaintiff and Class Members as a result of the Data Breach, which does not adequately address the lifelong harm that victims face following the Data Breach. Indeed, the Data Breach involves PII that cannot be changed, such as Social Security numbers.

53. The Notice Letters stated PII, including full names, Social Security numbers, addresses, driver's license numbers, state identification numbers, passport numbers, financial account information, health insurance information, and medical information were accessed and exfiltrated in the Data Breach.

54. As a result of the Data Breach, Plaintiff and 129,611 Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack and the substantial and imminent risk of identity theft.

55. Defendant waited over over 7 months to disclose the Data Brach to Plaintiff and Class Members. As a result of this delay, Plaintiff and Class Members had no idea their PII had been compromised in the Data Breach, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

56. Defendant's failure to timely detect and report the Data Breach made its consumers and employees vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

57. This PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiff and Class Members.

58. Despite recognizing its duty to do so, on information and belief, Defendant has not implemented reasonable cybersecurity safeguards or policies to protect its consumers' or employees' PII or trained its IT or data security employees to prevent, detect, and stop breaches of its systems. As a result, Defendant leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to consumers' PII.

59. Plaintiff and Class Members directly or indirectly entrusted Defendant with sensitive and confidential information, including their PII which includes information that is static, does not change, and can be used to commit myriad financial crimes.

60. Plaintiff and Class Members relied on Defendant to keep their PII confidential and securely maintained, to use their PII for authorized purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand Defendant safeguard their PII.

61. The unencrypted PII of Plaintiff and Class Members will likely end up for sale on the dark web as that is the *modus operandi* of hackers. Indeed, the Cactus cybercriminal ransomware gang, the hackers claiming to be responsible, posted Americold information would be coming soon.

62. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. In turn, unauthorized individuals can easily access the PII of Plaintiff and Class Members.

63. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiff and Class Members, causing the exposure of PII.

The Data Breach Was Foreseeable

64. Defendant should be keenly aware that its computer systems were a target for cyber security attacks as it reported to the SEC that it suffered cybersecurity attack in 2020.[16]

65. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in many industries preceding the date of the breach.

[16]https://www.sec.gov/ix?doc=/Archives/edgar/data/1455863/000119312520294943/d62059d8k.htm (last visited Dec. 13, 2023).

66. Because Defendant had duties to protect Plaintiff's and Class Members' PII, Defendant should have accessed readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

67. In the years immediately preceding the Data Breach, Defendant knew or should have known that Americold's computer systems and network were a target for cybersecurity attacks, including attacks involving data theft, because warnings were readily available and accessible via the internet. In addition to articles in the public press about the extensive number of data breaches affecting companies throughout all industries, governmental agencies have constantly sent and published notices of the need for companies who maintain sensitive personal information to carefully safeguard the sensitive and valuable information collected from consumers.

68. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[17]

69. Indeed, cyberattacks on large corporation like Americold have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential

[17] *See* 2021 Data Breach Annual Report, ITRC 6 (Jan. 2022), available at https://www.idtheftcenter.org/notified (last visited Dec. 13, 2023).

targets, so they are aware of, and prepared for, potential attack.[18]

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

71. Prior to the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack.

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

Defendant Had an Obligation to Protect the PII

73. Defendant's failure to adequately secure Plaintiff's and Class Members' PII breaches duties it owes Plaintiff and Class Members under statutory and common law. Moreover, Plaintiff and Class Members surrendered their highly

[18] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited Dec. 13, 2023).

sensitive personal data to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard its data, independent of any statute.

74. Defendant was prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. S*ee, e.g.*, *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

75. Therefore, the increase in such attacks, and the attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

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

adequately protected the PII of Plaintiff and Class Members.

77. Defendant owed a duty to Plaintiff and Class Members to design, maintain, and test its computer systems, servers, and networks to ensure that the PII in its possession was adequately secured and protected.

78. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII in its possession, including not sharing information with other entities who maintained substandard data security systems.

79. Defendant owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach on its data security systems in a timely manner.

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

81. Defendant owed a duty to Plaintiff and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII from theft because such an inadequacy would be a material fact in the decision to entrust this PII to Defendant.

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

83. Defendant owed a duty to Plaintiff and Class Members to encrypt

and/or more reliably encrypt Plaintiff's and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

84. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

85. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to, at least, tens of thousands of individuals' PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

Value of PII

86. The PII of individuals remains of high value to criminals, as evidenced by the prices criminals will pay through the Dark Web. Numerous sources cite Dark Web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[19] Experian reports that a stolen credit or debit card number can sell for

[19] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Dec. 13, 2023).

$5 to $110 on the dark web.[20] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[21]

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

88. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[22]

89. Among other forms of fraud, identity thieves may obtain driver's

---

[20] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Dec. 13, 2023).

[21] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Dec. 13, 2023).

[22] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Dec. 13, 2023).

licenses, government benefits, medical services, and housing or even give false information to police.

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

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data has been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[23]

91. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

92. Plaintiff and Class Members now face a lifetime of constant surveillance of their financial and personal records, credit monitoring, and loss of

[23] *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited Dec. 13, 2023).

rights. Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

93. Defendant has acknowledged the risk and harm caused to Plaintiff and Class Members as a result of the Data Breach. Defendant, to date, has offered Plaintiff and Class Members abbreviated, non-automatic credit monitoring services. The limited credit monitoring is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here. Moreover, Defendant put the burden squarely on Plaintiff and Class Members to enroll in the inadequate monitoring services.

Defendant Failed to Properly Protect Plaintiff's and Class Members' PII

94. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the PII of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially for individuals with whom it had not had a relationship for a period of time.

95. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure sensitive data they possess.

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

97. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[24]

98. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for their respective lifetimes.

99. To prevent and detect unauthorized cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from

[24] *See generally Fighting Identity Theft With the Red Flags Rule: A How-To Guide for Business*, FED. TRADE COMM., https://www.ftc.gov/business-guidance/resources/fighting-identity-theft-red-flags-rule-how-guide-business (last visited Dec. 13, 2023).

reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[25]

100. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's

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

> security to ensure the information you submit is encrypted before you provide it….
>
> - **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
>
> - **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
>
> - **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[26]

101. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

> **Secure internet-facing assets**
>
> - Apply latest security updates;
> - Use threat and vulnerability management;
> - Perform regular audit; remove privileged credentials;

[26] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://www.cisa.gov/news-events/news/protecting-against-ransomware (last visited Dec. 13, 2023).

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities;
- Hunt for brute force attempts;
- Monitor for cleanup of Event Logs;
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall;
- Enable tamper protection;
- Enable cloud-delivered protection;
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[27]

102. Moreover, given that Defendant was storing the PII of Plaintiff and

[27] *See Human-operated ransomware attacks: A preventable disaster*, Microsoft (Mar. 5, 2020). https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Dec. 13, 2023).

Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

103. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the PII of Plaintiff and Class Members.

104. As a result of computer systems in need of security upgrades, inadequate procedures for handling email phishing attacks, viruses, malignant computer code, hacking attacks, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII.

105. Because Defendant failed to properly protect and safeguard Plaintiff's and Class Members' PII, an unauthorized third party was able to access Defendant's network, and access Defendant's database and system configuration files and exfiltrate that data.

Defendant Failed to Comply with Industry Standards

106. As shown above, experts studying cyber security routinely identify companies in the logistics industry as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

107. Several best practices have been identified that at a minimum should be implemented by logistic and warehousing providers like Defendant, including, but

not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

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

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

110. The foregoing frameworks are existing and applicable industry standards in the logistics industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

111. Upon information and belief, Defendant failed to comply with one or more of the foregoing industry standards.

Defendant's Negligent Acts and Breaches

112. Defendant participated in and controlled the process of gathering the PII from Plaintiff and Class Members.

113. Defendant therefore assumed and otherwise owed duties and obligations to Plaintiff and Class Members to take reasonable measures to protect the information, including the duty of oversight, training, instruction, testing of the data security policies and network systems. Defendant breached these obligations to Plaintiff and Class Members and/or was otherwise negligent because it failed to properly implement data security systems and policies that would adequately safeguard Plaintiff's and Class Members' PII. Upon information and belief, Defendant's unlawful conduct included, but is not limited to, one or more of the following acts and/or omissions:

a. Failing to design and maintain an adequate data security system to reduce the risk of data breaches and protect Plaintiff's and Class Members' PII;

b. Failing to properly monitor its data security systems for data security vulnerabilities and risk;

c. Failing to test and assess the adequacy of its data security system;

d. Failing to develop adequate training programs related to the proper handling of emails and email security practices;

e. Failing to develop and put into place uniform procedures and data security protections for its network;

f. Failing to adequately fund and allocate resources for the adequate design, operation, maintenance, and updating necessary to meet industry standards for data security protection;

g. Failing to ensure or otherwise require that it was compliant with FTC guidelines for cybersecurity;

h. Failing to ensure or otherwise require that it was adhering to one or more of industry standards for cybersecurity discussed above;

i. Failing to implement or update antivirus and malware protection software in need of security updating;

j. Failing to require encryption or adequate encryption on its data systems;

k. Otherwise negligently and unlawfully failing to safeguard Plaintiff's and Class Members' PII provided to Defendant, which in turn allowed cyberthieves to access its IT systems.

COMMON INJURIES & DAMAGES

114. As result of Defendant's ineffective and inadequate data security practices, Plaintiff and Class Members now face a present and ongoing risk of fraud and identity theft.

115. Due to the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) "out of pocket" costs incurred mitigating the materialized risk and imminent threat of

identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) diminution or loss of value of their PII; and (i) the continued risk to their PII, which remains in Defendant's possession, and which is subject to further breaches, so long as Defendant fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

The Risk of Identity Theft to Plaintiff and Class Members Is Present and Ongoing

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

117. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity – or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

118. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches are often the starting point for these additional targeted attacks on the victims.

119. The Dark Web is an unindexed layer of the internet that requires special software or authentication to access.[28] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, Dark Web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[29] This prevents Dark Web marketplaces from being easily monitored by authorities or accessed by those not in the know.

[28]Louis DeNicola, *What Is the Dark Web?*, Experian (May 12, 2021), https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last visited Dec. 13, 2023).

[29] *Id.*

120. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal, and medical information like the PII at issue here.[30] The digital character of PII stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth, and medical information.[31] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[32]

121. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they are immutable and may be put to numerous serious 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

[30] *What is the Dark Web?* – Microsoft 365 (July 15, 2022), https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web (last visited Dec. 13, 2023).

[31] *Id.*; *see also* Louis DeNicola, *supra* note 25.

[32] *Id.*

fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[33]
>
> What's more, it is no 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. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

122. 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."[34]

123. Identity thieves can also use Social Security numbers to obtain a

[33] Social Security Administration, *Identity Theft and Your Social Security Number* (2021), available at: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Dec. 13, 2023).

[34] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (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 Dec. 13, 2023).

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. 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 personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. And the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[35]

124. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.[36]

125. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[37] Defendant did not rapidly report to Plaintiff and Class Members that their

[35] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2021), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Dec. 13, 2023).

[36] *See 2019 Internet Crime Report*, FBI (Feb. 11, 2020), https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120 (last visited Dec. 13, 2023).

[37] *Id.*

PII had been stolen.

126. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

127. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

128. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PII. To protect themselves, Plaintiff and Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

129. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable.

Data is currency. The larger the data set, the greater potential for analysis and profit."[38]

130. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[39]

131. According to the FTC, unauthorized PII disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money, and patience to resolve the fallout. The FTC treats the failure to employ

[38] Statement of FTC Commissioner Pamela Jones Harbour (Remarks Before FTC Exploring Privacy Roundtable), FTC (Dec. 7, 2009), http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf (last visited Dec. 13, 2023).

[39] *See generally* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Dec. 13, 2023).

reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act.[40]

132. Defendant's failure to properly notify Plaintiff and Class Members of the Data Breach exacerbated Plaintiff's and Class Members' injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

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

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

134. Thus, due to Defendant's admitted recognition of the actual and imminent risk of identity theft, Defendant offered Plaintiff and Class Members abbreviated, limited, and non-automatic credit monitoring services.

---

[40] *See, e.g., Protecting Personal Information: A Guide for Business*, FTC, https://www.ftc.gov/news-events/news/press-releases/2016/07/commission-finds-labmd-liable-unfair-data-security-practices (last visited Dec. 13, 2023).

135. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing, or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

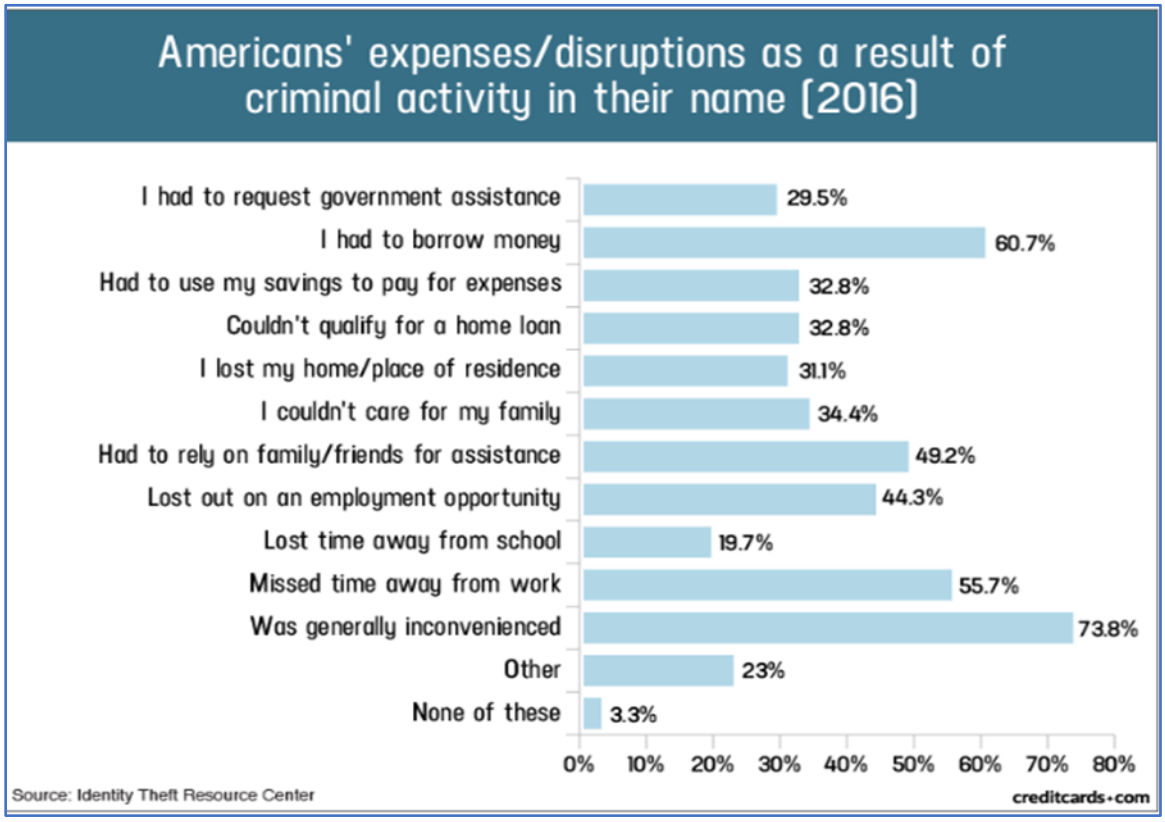
136. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[41]

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

[41] *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-07-737, PERSONAL INFORMATION: DATA BREACHES ARE FREQUENT, BUT EVIDENCE OF RESULTING IDENTITY THEFT IS LIMITED; HOWEVER, THE FULL EXTENT IS UNKNOWN (2007) ("GAO Report"), available at https://www.gao.gov/new.items/d07737.pdf (last visited Dec. 13, 2023).

credit, and correcting their credit reports.[42]

138. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[43]



139. Indeed, the FTC recommends that identity theft victims take several steps and spend time to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider

---

[42] *See* Federal Trade Commission, IdentityTheft.gov, https://www.identitytheft.gov/Steps (last visited Dec. 13, 2023).

[43] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://web.archive.org/web/20190304002224/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited Dec. 13, 2023).

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, placing a credit freeze on their credit, and correcting their credit reports.[44]

Diminution of Value of the PII

140. PII is a valuable property right.[45] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

141. For example, drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase PII on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves.

142. PII can sell for as much as $363 per record according to the Infosec

[44] *See* Federal Trade Commission, IdentityTheft.gov, https://www.identitytheft.gov/Steps (last visited Dec. 13, 2023).

[45] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, 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).

Institute.[46]

143. Medical information is especially valuable to identity thieves. Cybersecurity firm Trustwave calculated the black-market value of medical records at $250 each.[47]

144. An active and robust legitimate marketplace for PII also exists. In 2019, the data brokering industry was worth roughly $200 billion.[48] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[49, 50]Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[51]

---

[46] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Dec. 13, 2023).

[47] Paul Ndrag, *Medical records are the hottest items on the dark web*, Fierce Healthcare (Jan. 26, 2021), https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web (last visited Dec. 13, 2023).

[48] David Lazarus, *Column: Shadowy data brokers make the most of their invisibility cloak*, LA Times (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Dec. 13, 2023).

[49] https://datacoup.com/ (last visited Dec. 13, 2023).

[50] https://digi.me/questions/what-is-a-digi-me-personal-data-vault (last visited Dec. 13, 2023).

[51] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Dec. 13, 2023).

145. As a result of the Data Breach, Plaintiff's and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release onto the Dark Web, where it may soon be available and holds significant value for the threat actors.

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

146. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered as a result of the Data Breach.

147. The abbreviated, limited, and non-automatic credit monitoring offered to Plaintiff and Class Members whose PII was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face ongoing identity theft and financial fraud for the remainder of their lives. Defendant also places the burden squarely on Plaintiff and Class Members by requiring them to independently sign up for that service, as opposed to automatically enrolling all victims of this Data Breach.

148. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/Dark Web for sale and purchase by criminals intending

to utilize the PII for identity theft crimes – e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

149. It must 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 PII and/or financial information is stolen and when it is used.

150. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his 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.

151. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts.[52] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

[52] *See* Jesse Damiani, *Your Social Security Number Costs $4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1 (last visited Dec. 13, 2023

152. Consequently, Plaintiff and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

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

Injunctive Relief Is Necessary to Protect against Future Data Breaches

154. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing PII is not accessible online and that access to such data is password protected.

Plaintiff's Individual Experience

Plaintiff Lamont Bracy's Experience

155. At the time of the Data Breach, Defendant retained Plaintiff Bracy's PII in its system.

156. Plaintiff Bracy was sent a Notice Letter dated December 8, 2023,

informing him that Defendant had experienced a Data Breach and that Plaintiff's PII, that may have included his full name, Social Security number, address, driver's license number, state identification number, passport number, financial account information, health insurance information, and medical information were compromised in the breach.

157. As a result of the Data Breach, Plaintiff Bracy spent time dealing with the consequences of the Data Breach, which includes placing a security freeze on his credit reports, verifying the legitimacy of the Notice of Data Breach, self-monitoring his accounts and/or credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured. Moreover, this time was spent at Defendant's direction by way of the Notice Letter where Defendant advised Plaintiff Bracy to mitigate his damages by, among other things, freezing his credit accounts and monitoring his accounts for fraudulent activity.

158. Plaintiff Bracy is a cautious person and is therefore very careful about sharing his sensitive PII. As a result, he has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff Bracy stores any documents containing his PII in a safe and secure location or destroys the documents. Moreover, Plaintiff Bracy diligently chooses unique usernames and passwords for his various online accounts, changing and refreshing them as needed to ensure his information is as protected as it can be.

159. The Data Breach caused Plaintiff Bracy to suffer a loss of privacy.

160. Plaintiff Bracy has also experienced an increase in the number of spam calls and emails since the Data Breach.

161. The Data Breach has caused Plaintiff Bracy to suffer imminent and impending injury arising from the substantially increased risk of additional future fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

162. The loss of privacy and substantial present risk of additional imminent harm have caused Plaintiff Bracy to suffer stress, fear, and anxiety as Plaintiff Bracy is very concerned that his sensitive PII is now in the hands of data thieves and shall remain that way for the remainder of his lifetime and there is nothing Plaintiff Bracy can do to retrieve his stolen PII from the cyber-criminals.

163. Plaintiff Bracy is aware of no other source from which the theft of his PII could have come. He regularly takes steps to safeguard his own PII within his own control.

164. Given the time Plaintiff Bracy has lost investigating this Data Breach, taking steps to understand its full scope, determining the appropriate remedial steps, contacting counsel, etc., coupled with Plaintiff Bracy's resultant and naturally foreseeable fears/concerns for the use of Plaintiff Bracy's valuable PII, the damages articulated more specifically above are far from the full extent of the harm thereto.

CLASS ALLEGATIONS

165. Plaintiff brings this nationwide class action on behalf of himself and on behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

166. The nationwide Class that Plaintiff seeks to represent is defined as follows:

> **All United States residents who were sent a Notice Letter by Defendant Americold Logistics LLC notifying them that their PII was compromised in the Data Breach.**

167. The nationwide Class is referred to herein as the "Class."

168. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

169. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

170. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous

that joinder of all members is impracticable. Upon information and belief, there are at least multiple thousands of individuals who were notified by Defendant of the Data Breach. According to the report submitted to the Maine Attorney General's office, 129,611 individuals had their PII compromised in this Data Breach.[53] The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

171. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendant had duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendant had duties not to use the PII of Plaintiff and Class Members for non-business purposes;

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

e. Whether and when Defendant actually learned of the Data Breach;

[53] *See* Data Breach Notifications, Office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/80071f08-cdaa-4ca5-8efb-a2bf28c33fe5.shtml (last visited Dec. 13, 2023).

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

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

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

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

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

k. Whether Defendant violated the consumer protection statutes invoked herein;

l. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

m. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

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

Data Breach.

172. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

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

174. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

175. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

176. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is

representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

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

178. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

179. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

180. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

181. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the

resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;

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

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

CAUSES OF ACTION

COUNT I
NEGLIGENCE AND NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

182. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in 1 through 181.

183. Plaintiff and the Class entrusted Defendant with their PII.

184. Plaintiff and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

185. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

186. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the

Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

187. Defendant 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 Defendant's security protocols to ensure that the PII of Plaintiff and the Class in Defendant's possession was adequately secured and protected.

188. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain.

189. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Class.

190. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant, either directly or indirectly, with their confidential PII, a necessary part of obtaining services from Defendant.

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

192. A breach of security, unauthorized access, and resulting injury to

Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

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

194. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

195. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

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

197. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were

compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

198. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Class.

199. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

200. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Class during the time the PII was within Defendant's possession or control.

201. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

202. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Class in the face of increased risk of theft.

203. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place

to detect and prevent dissemination of PII.

204. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove PII that it was no longer required to retain pursuant to regulations.

205. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

206. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Nationwide Class, the PII of Plaintiff and the Class would not have been compromised.

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

208. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form

part of the basis of Defendant's duty in this regard.

209. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

210. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

211. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

212. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

213. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses

associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

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

215. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to

further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

216. As a direct and proximate result of Defendant's negligence, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiff and the Class)

217. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in 1 through 181.

218. The PII of Plaintiff and Class Members, including full names and Social Security numbers, was provided and entrusted to Defendant.

219. Plaintiff and Class Members provided their PII to Defendant, either directly or indirectly, through Defendant's clients, as part of Defendant's regular business practices.

220. Plaintiff and the Class entrusted their PII to Defendant. In doing so, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen. As a condition of obtaining services and being employed by Defendant's clients, Plaintiff and Class Members provided and entrusted their PII. In so doing, Plaintiff and Class Members

entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

221. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PII to Defendant and/or Defendant's clients with the reasonable understanding that their PII would be adequately protected by any business associates, like Defendant, from foreseeable threats. This inherent understanding exists independent of any other law or contractual obligation any time that highly sensitive PII is exchanged as a condition of receiving services. It is common sense that but for this implicit and/or explicit agreement, Plaintiff and Class Members would not have provided their PII.

222. Defendant separately has contractual obligations arising from and/or supported by the consumer facing statements in its Privacy Policy.

223. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

224. Defendant breached the implied contracts it made with Plaintiff and Class Members by failing to safeguard and protect their PII and by failing to provide timely and accurate notice that PII was compromised as a result of the Data Breach.

225. As a direct and proximate result of Defendant's above-described breach

of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

226. As a result of Defendant's breach of implied contract, Plaintiff and Class Members are entitled to and demand actual, consequential, and nominal damages.

COUNT III
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Class)

227. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in 1 through 181. Notwithstanding, Plaintiff brings this claim in the alternative to any claim for breach of contractual obligations.

228. Defendant benefited from receiving Plaintiff's and Class Members' PII by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

229. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

230. Defendant was also enriched from the value of Plaintiff's and Class Members' PII. PII has independent value as a form of intangible property. Defendant also derives value from this information because it allows Defendant to operate its business and generate revenue.

231. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

232. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

233. Defendant acquired the monetary benefit and PII through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

234. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

235. Plaintiff and Class Members have no adequate remedy at law.

236. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

237. As a direct and proximate result of Defendant's conduct, Plaintiff and

Class Members have suffered and will continue to suffer other forms of injury and/or harm.

238. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them.

COUNT IV
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

239. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in 1 through 181.

240. Plaintiff and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

241. Defendant owed a duty to Plaintiff and Class Members to keep this information confidential.

242. The unauthorized acquisition (*i.e.*, theft) by a third party of Plaintiff and Class Members' PII is highly offensive to a reasonable person.

243. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

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

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

246. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and Class Members.

247. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiff and the Class was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and Class Members to suffer damages.

248. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and Class Members since their PII is still maintained by Defendant with its inadequate cybersecurity system and policies.

249. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's

inability to safeguard their PII.

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

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

COUNT V
VIOLATION OF O.C.G.A. § 13-6-11
(On Behalf of Plaintiff Bracy and the Class)

252. Plaintiff Bracy re-alleges and incorporates by reference herein all of the allegations contained in 1 through 181.

253. Defendant through its actions alleged and described herein acted in bad faith, was stubbornly litigious, or caused Plaintiff and the Class unnecessary trouble and expense with respect to the events underlying this litigation.

254. 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 companies such as Defendant for failing to implement and use reasonable measures to protect PII.

255. Defendant violated Section 5 of the FTC ACT by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII that it obtained and stored and the foreseeable consequences of a data breach.

256. Defendant also has a duty under the Georgia Constitution ("the Constitution") which contains a Right to Privacy Clause, Chapter 1, Article 1, to protect its users' private information. The Georgia Constitution states, "no person shall be deprived of life, liberty, or property except by due process of law." Moreover, the Georgia Constitution identifies certain invasions of privacy, including the Public Disclosure of Private Life which prohibits the public disclosure of private facts.

257. This duty has been recognized by the Georgia Supreme Court in the Restatement of the Law of Torts (Second) §652A which specifically recognized four common law invasion of privacy claims in Georgia, which include 1) appropriation of likeness; 2) intrusion on solitude or seclusion; 3) public disclosure of private facts; and 4) false light.

258. Defendant's implementation of inadequate data security measures, its failure to resolve vulnerabilities and deficiencies, and its abdication of its

responsibility to reasonably protect data it required Plaintiff and the Class to provide and store on its own servers constitutes a violation of the Georgia Constitution and the Restatement of the Law of Torts (Second).

259. Defendant knew or should have known that it had a responsibility to protect the PII it required Plaintiff and the Class to provide and stored, that it was entrusted with this PII, and that it was the only entity capable of adequately protecting the PII.

260. Despite that knowledge, Defendant abdicated its duty to protect the PII it required Plaintiff and the Class to provide and that it stored.

261. As a direct and proximate result of Defendant's actions, Plaintiff's and the Class Members' PII was stolen. As further alleged above, the Data Breach was a direct consequence of Defendant's abrogation of data security responsibility and its decision to employ knowingly deficient data security measures that knowingly left the PII unsecured. Had Defendant adopted reasonable data security measures, it could have prevented the Data Breach.

262. As further described above, Plaintiff and the Class have been injured and suffered losses directly attributable to the Data Breach.

263. Plaintiff and the Class therefore request that their claim for recovery of expenses of litigation and attorneys' fees be submitted to the jury, and that the Court enter a judgment awarding their expenses of litigation and attorneys' fees pursuant

to O.C.G.A. § 13-6-11.

COUNT VI
GEORGIA UNIFORM DECEPTIVE TRADE PRACTICES ACT
O.C.G.A. §§ 13-1-370, *et seq.*

264. Plaintiff Bracy re-alleges and incorporates by reference herein all of the allegations contained in 1 through 181.

265. Defendant, Plaintiff, and Class Members are "persons within the meaning of § 10-1-371(5) of the Georgia Uniform Deceptive Trade Practices Act ("Georgia UDTPA").

266. Defendant engaged in deceptive trade practices in the conduct of its business in violation of O.C.G.A. § 10-1-372(a), which states in pertinent part that it is a deceptive trade practice to:

> (a)(5) Represent[] that goods or services have sponsorship, approval, characteristics, . . . uses, [or] benefits . . . that they do not have;
>
> (a)(7) Represent[] that goods or services are of a particular standard, quality, or grade . . . if they are of another; or
>
> (a)(12) Engage[] in any other conduct which similarly creates a likelihood of confusion or of misunderstanding.

267. Defendant engaged in deceptive trade practices in violation of the Georgia DTPA, Ga. Code Ann. § 10-1-372(a)(5), (7), and (12), by, among other things:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Class Members' PII, which was a direct

and proximate cause of the Data Breach;

b. Making implied or implicit representations that its data security practices were sufficient to protect Plaintiff's and Class Members' PII. Defendant made implied or implicit representations that its data security practices were sufficient to protect Plaintiff's and Class Members' PII. By virtue of accepting Plaintiff's and Class Members' PII, Defendant implicitly represented that its data security processes were sufficient to safeguard the PII;

c. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

d. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

e. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Class Members' PII, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII,

including duties imposed by the FTC Act, 15 U.S.C. § 45;

g. Failing to timely and adequately notify Plaintiff and Class Members of the Data Breach;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Class Members' PII; and

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

268. Because Defendant required Plaintiff and Class Members to provide their PII as a prerequisite for services from Defendant, Plaintiff and Class Members reasonably expected that Defendant's data security and data storage systems were adequately secure to protect their PII.

269. Defendant's representations and omissions were material because they were likely to deceive reasonable persons about the adequacy of Defendant's data security and ability to protect the confidentiality of Plaintiff's and Class Members' PII.

270. Defendant intended to mislead Plaintiff and Class Members and induce them to rely on its misrepresentations and omissions.

271. Plaintiff and Class Members relied on Defendant to advise them if their

data security and data storage systems were not adequately secure to protect their PII.

272. Plaintiff and Class Members had no opportunity to make any inspection of Defendant's data security practices or to otherwise ascertain the truthfulness of Defendant's representations and omissions regarding data security, including Defendant's failure to alert Plaintiff and Class Members that their data security and data storage systems were not adequately secure and, thus, were vulnerable to attack.

273. Plaintiff and Class Members relied to their detriment on Defendant's misrepresentations and deceptive omissions regarding their data security practices.

274. Had Defendant disclosed that its data security and data storage systems were not secure, and thus, vulnerable to attack, Plaintiff and Class Members would not have entrusted Defendant with their PII.

275. Defendant acted intentionally, knowingly, and maliciously to violate the Georgia UDTPA, and recklessly disregarded Plaintiff's and Class Members' rights. Past data breaches in the industry put Defendant on notice that its security and privacy protections were inadequate.

276. Had Defendant disclosed to Plaintiff and Class Members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business, and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, Defendant was trusted with

sensitive and valuable PII regarding thousands of persons, including Plaintiff the Class. Defendant accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because Defendant held itself out as maintaining a secure platform for PII, Plaintiff and the Class acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

277. As a direct and proximate result of Defendant's unfair and deceptive business practices, Plaintiff and Class Members suffered ascertainable losses, including but not limited to, a loss of privacy, the loss of the benefit of their bargain, out-of-pocket monetary losses and expenses, the value of their time reasonable incurred to remedy or mitigate the effects of the Data Breach, the loss of value of their PII, the imminent and substantially increased risk of fraud and identity theft, and the need to dedicate future expenses and time to protect themselves against further loss.

278. To date, Defendant has not provided sufficient details regarding the full scope of the Data Breach, or any details related to the remedial measures it has taken to improve its data security practices and more fully safeguard Plaintiff's and Class Members' PII from future compromise. As a result, Plaintiff and Class Members remain uninformed and confused as to the adequacy of Defendant's data security and Defendant's ability to protect the PII entrusted to it. Without adequate

improvements, Plaintiff's and Class Members' PII remains at an unreasonable risk of future compromise.

279. Defendant, through its omissions and its Data Breach Notice Letters, continues to represent and imply that its data security measures are adequate to protect Plaintiff's and Class Members' PII. Such continued representations and implications, without disclosure of the full scope of the Data Breach or Defendant's subsequent remedial enhancements, place Plaintiff and Class Members at a future risk of harm, as Plaintiff and Class Members are not fully informed as to whether Defendant's data security measures have been improved since the Data Breach. By all available measures, Defendant's data security practices and systems have not been adequately improved, and Plaintiff and Class Members remain at an unreasonable risk from future cyberattacks.

280. Plaintiff and the Class are therefore entitled to the injunctive relief sought herein, because, among other things, Defendant continues to retain their PII, future cyber-attacks targeting the same data are foreseeable, and Defendant has not provided sufficient notice identifying any remedial measures that will protect the data from future attack. Moreover, absent injunctive relief, Defendant will continue to misrepresent and imply that its data security practices and systems are adequate to protect the PII of Plaintiff and Class Members from future cyberattacks without providing any firm details or basis to support these representations.

281. The Georgia DTPA states that the "court, in its discretion, may award attorney's fees to the prevailing party if . . . [t]he party charged with a deceptive trade practice has willfully engaged in the trade practice knowing it to be deceptive." Ga. Code Ann. § 10-1-373(b)(2). Defendant willfully engaged in deceptive trade practices knowing them to be deceptive. Defendant knew or should have known that its data security practices were deficient. Defendant was aware that entities responsible for collecting and maintaining large amounts of Private Information, including Social Security numbers, are frequent targets of sophisticated cyberattacks. Defendant knew or should have known that its data security practices were insufficient to guard against those attacks.

282. The Georgia DTPA states that "[c]osts shall be allowed to the prevailing party unless the court otherwise directs." Ga. Code Ann. § 10-1-373(b). Plaintiff and the Class are entitled to recover their costs of pursuing this litigation.

283. Plaintiff and Class Members seek all monetary and non-monetary relief allowed by the Georgia DTPA, including injunctive relief and attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Classes, and appointing Plaintiff and his Counsel to represent the Class;

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

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

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

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

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

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

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

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

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

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

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to

other portions of Defendant's systems;

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

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

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

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

xiv. requiring Defendant to implement, maintain, regularly review, and

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

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

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including, but not limited to, actual, consequential, and nominal damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses pursuant

to O.C.G.A. Section 13-6-11 and as allowed by law;

F. For prejudgment interest on all amounts awarded; and

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

DEMAND FOR JURY TRIAL

A jury trial is demanded by Plaintiff and the putative Class Members as to all issues so triable.

Date: December 14, 2023.

Respectfully Submitted,

/s/MaryBeth V. Gibson
MaryBeth V. Gibson
Georgia Bar No. 725843
N. Nickolas Jackson
Georgia Bar No. 841433
THE FINLEY FIRM, P.C.
3535 Piedmont Rd.
Building 14, Suite 230
Atlanta, GA 30305
Phone: (678) 642-2503
Fax: (404) 320-9978
mgibson@thefinleyfirm.com
njackson@thefinleyfirm.com

Terence R. Coates (*pro hac vice forthcoming*)
Justin C. Walker (*pro hac vice forthcoming*)
MARKOVITS, STOCK & DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, OH 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
jwalker@msdlegal.com

Counsel for Plaintiff and Putative Class

CERTIFCATE OF COMPLIANCE

I certify that the foregoing pleading has been prepared with Times New Roman, 14-point font, in compliance with L.R. 5.1B.

/s/ MaryBeth V. Gibson
MaryBeth V. Gibson

JS44 (Rev. 10/2020 NDGA)

CIVIL COVER SHEET

The JS44 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 is required for the use of the Clerk of Court for the purpose of initiating the civil docket record. (SEE INSTRUCTIONS ATTACHED)

I. (a) PLAINTIFF(S)

LAMONT BRACY, on behalf of himself and all others similarly situated

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF Montgomery, AL
(EXCEPT IN U.S. PLAINTIFF CASES)

DEFENDANT(S)

AMERICOLD LOGISTICS LLC

COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT Fulton
(IN U.S. PLAINTIFF CASES ONLY)

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

(c) ATTORNEYS (FIRM NAME, ADDRESS, TELEPHONE NUMBER, AND E-MAIL ADDRESS)

MaryBeth V. Gibson and N. Nickolas Jackson
The Finley Firm, P.C.
3535 Piedmont Road
Bldg 14, Suite 230
Atlanta, Georgia 30305
404-320-9979

ATTORNEYS (IF KNOWN)

II. BASIS OF JURISDICTION

(PLACE AN "X" IN ONE BOX ONLY)

- ☐ 1 U.S. GOVERNMENT PLAINTIFF
- ☐ 3 FEDERAL QUESTION (U.S. GOVERNMENT NOT A PARTY)
- ☐ 2 U.S. GOVERNMENT DEFENDANT
- ☑ 4 DIVERSITY (INDICATE CITIZENSHIP OF PARTIES IN ITEM III)

III. CITIZENSHIP OF PRINCIPAL PARTIES

(PLACE AN "X" IN ONE BOX FOR PLAINTIFF AND ONE BOX FOR DEFENDANT)
(FOR DIVERSITY CASES ONLY)

PLF	DEF		PLF	DEF	
☐ 1	☐ 1	CITIZEN OF THIS STATE	☐ 4	☑ 4	INCORPORATED OR PRINCIPAL PLACE OF BUSINESS IN THIS STATE
☑ 2	☐ 2	CITIZEN OF ANOTHER STATE	☐ 5	☐ 5	INCORPORATED AND PRINCIPAL PLACE OF BUSINESS IN ANOTHER STATE
☐ 3	☐ 3	CITIZEN OR SUBJECT OF A FOREIGN COUNTRY	☐ 6	☐ 6	FOREIGN NATION

IV. 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 District)
- ☐ 6 MULTIDISTRICT LITIGATION - TRANSFER
- ☐ 7 APPEAL TO DISTRICT JUDGE FROM MAGISTRATE JUDGE JUDGMENT
- ☐ 8 MULTIDISTRICT LITIGATION - DIRECT FILE

V. CAUSE OF ACTION (CITE THE U.S. CIVIL STATUTE UNDER WHICH YOU ARE FILING AND WRITE A BRIEF STATEMENT OF CAUSE - DO NOT CITE JURISDICTIONAL STATUTES UNLESS DIVERSITY)

28 U.S.C. Section 1332(d)(2)(A). This is a class action filed by Plaintiff and all others similarly situated for Data Breach that happened due to Defendant's failure to safeguard Plainitff's protected personally identifiable information. Suit for damages and other relief for negligence and negligence per se resulting from data breach, declaratory and injunctive relief.

(IF COMPLEX, CHECK REASON BELOW)

- ☐ 1. Unusually large number of parties.
- ☐ 2. Unusually large number of claims or defenses.
- ☐ 3. Factual issues are exceptionally complex
- ☐ 4. Greater than normal volume of evidence.
- ☐ 5. Extended discovery period is needed.
- ☐ 6. Problems locating or preserving evidence
- ☐ 7. Pending parallel investigations or actions by government.
- ☐ 8. Multiple use of experts.
- ☐ 9. Need for discovery outside United States boundaries.
- ☐ 10. Existence of highly technical issues and proof.

CONTINUED ON REVERSE

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT $ _____ APPLYING IFP _____ MAG. JUDGE (IFP) _____

JUDGE _____ MAG. JUDGE _____ (Referral) NATURE OF SUIT _____ CAUSE OF ACTION _____

VI. NATURE OF SUIT (PLACE AN "X" IN ONE BOX ONLY)

CONTRACT - "0" MONTHS DISCOVERY TRACK
- ☐ 150 RECOVERY OF OVERPAYMENT & ENFORCEMENT OF JUDGMENT
- ☐ 152 RECOVERY OF DEFAULTED STUDENT LOANS (Excl. Veterans)
- ☐ 153 RECOVERY OF OVERPAYMENT OF VETERAN'S BENEFITS

CONTRACT - "4" MONTHS DISCOVERY TRACK
- ☐ 110 INSURANCE
- ☐ 120 MARINE
- ☐ 130 MILLER ACT
- ☐ 140 NEGOTIABLE INSTRUMENT
- ☐ 151 MEDICARE ACT
- ☐ 160 STOCKHOLDERS' SUITS
- ☐ 190 OTHER CONTRACT
- ☐ 195 CONTRACT PRODUCT LIABILITY
- ☐ 196 FRANCHISE

REAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☐ 210 LAND CONDEMNATION
- ☐ 220 FORECLOSURE
- ☐ 230 RENT LEASE & EJECTMENT
- ☐ 240 TORTS TO LAND
- ☐ 245 TORT PRODUCT LIABILITY
- ☐ 290 ALL OTHER REAL PROPERTY

TORTS - PERSONAL INJURY - "4" MONTHS DISCOVERY TRACK
- ☐ 310 AIRPLANE
- ☐ 315 AIRPLANE PRODUCT LIABILITY
- ☐ 320 ASSAULT, LIBEL & SLANDER
- ☐ 330 FEDERAL EMPLOYERS' LIABILITY
- ☐ 340 MARINE
- ☐ 345 MARINE PRODUCT LIABILITY
- ☐ 350 MOTOR VEHICLE
- ☐ 355 MOTOR VEHICLE PRODUCT LIABILITY
- ☑ 360 OTHER PERSONAL INJURY
- ☐ 362 PERSONAL INJURY - MEDICAL MALPRACTICE
- ☐ 365 PERSONAL INJURY - PRODUCT LIABILITY
- ☐ 367 PERSONAL INJURY - HEALTH CARE/ PHARMACEUTICAL PRODUCT LIABILITY
- ☐ 368 ASBESTOS PERSONAL INJURY PRODUCT LIABILITY

TORTS - PERSONAL PROPERTY - "4" MONTHS DISCOVERY TRACK
- ☐ 370 OTHER FRAUD
- ☐ 371 TRUTH IN LENDING
- ☑ 380 OTHER PERSONAL PROPERTY DAMAGE
- ☐ 385 PROPERTY DAMAGE PRODUCT LIABILITY

BANKRUPTCY - "0" MONTHS DISCOVERY TRACK
- ☐ 422 APPEAL 28 USC 158
- ☐ 423 WITHDRAWAL 28 USC 157

CIVIL RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 440 OTHER CIVIL RIGHTS
- ☐ 441 VOTING
- ☐ 442 EMPLOYMENT
- ☐ 443 HOUSING/ ACCOMMODATIONS
- ☐ 445 AMERICANS with DISABILITIES - Employment
- ☐ 446 AMERICANS with DISABILITIES - Other
- ☐ 448 EDUCATION

IMMIGRATION - "0" MONTHS DISCOVERY TRACK
- ☐ 462 NATURALIZATION APPLICATION
- ☐ 465 OTHER IMMIGRATION ACTIONS

PRISONER PETITIONS - "0" MONTHS DISCOVERY TRACK
- ☐ 463 HABEAS CORPUS- Alien Detainee
- ☐ 510 MOTIONS TO VACATE SENTENCE
- ☐ 530 HABEAS CORPUS
- ☐ 535 HABEAS CORPUS DEATH PENALTY
- ☐ 540 MANDAMUS & OTHER
- ☐ 550 CIVIL RIGHTS - Filed Pro se
- ☐ 555 PRISON CONDITION(S) - Filed Pro se
- ☐ 560 CIVIL DETAINEE: CONDITIONS OF CONFINEMENT

PRISONER PETITIONS - "4" MONTHS DISCOVERY TRACK
- ☐ 550 CIVIL RIGHTS - Filed by Counsel
- ☐ 555 PRISON CONDITION(S) - Filed by Counsel

FORFEITURE/PENALTY - "4" MONTHS DISCOVERY TRACK
- ☐ 625 DRUG RELATED SEIZURE OF PROPERTY 21 USC 881
- ☐ 690 OTHER

LABOR - "4" MONTHS DISCOVERY TRACK
- ☐ 710 FAIR LABOR STANDARDS ACT
- ☐ 720 LABOR/MGMT. RELATIONS
- ☐ 740 RAILWAY LABOR ACT
- ☐ 751 FAMILY and MEDICAL LEAVE ACT
- ☐ 790 OTHER LABOR LITIGATION
- ☐ 791 EMPL. RET. INC. SECURITY ACT

PROPERTY RIGHTS - "4" MONTHS DISCOVERY TRACK
- ☐ 820 COPYRIGHTS
- ☐ 840 TRADEMARK
- ☐ 880 DEFEND TRADE SECRETS ACT OF 2016 (DTSA)

PROPERTY RIGHTS - "8" MONTHS DISCOVERY TRACK
- ☐ 830 PATENT
- ☐ 835 PATENT-ABBREVIATED NEW DRUG APPLICATIONS (ANDA) - a/k/a Hatch-Waxman cases

SOCIAL SECURITY - "0" MONTHS DISCOVERY TRACK
- ☐ 861 HIA (1395ff)
- ☐ 862 BLACK LUNG (923)
- ☐ 863 DIWC (405(g))
- ☐ 863 DIWW (405(g))
- ☐ 864 SSID TITLE XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS - "4" MONTHS DISCOVERY TRACK
- ☐ 870 TAXES (U.S. Plaintiff or Defendant)
- ☐ 871 IRS - THIRD PARTY 26 USC 7609

OTHER STATUTES - "4" MONTHS DISCOVERY TRACK
- ☐ 375 FALSE CLAIMS ACT
- ☐ 376 Qui Tam 31 USC 3729(a)
- ☐ 400 STATE REAPPORTIONMENT
- ☐ 430 BANKS AND BANKING
- ☐ 450 COMMERCE/ICC RATES/ETC.
- ☐ 460 DEPORTATION
- ☐ 470 RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS
- ☐ 480 CONSUMER CREDIT
- ☐ 485 TELEPHONE CONSUMER PROTECTION ACT
- ☐ 490 CABLE/SATELLITE TV
- ☐ 890 OTHER STATUTORY ACTIONS
- ☐ 891 AGRICULTURAL ACTS
- ☐ 893 ENVIRONMENTAL MATTERS
- ☐ 895 FREEDOM OF INFORMATION ACT 899
- ☐ 899 ADMINISTRATIVE PROCEDURES ACT / REVIEW OR APPEAL OF AGENCY DECISION
- ☐ 950 CONSTITUTIONALITY OF STATE STATUTES

OTHER STATUTES - "8" MONTHS DISCOVERY TRACK
- ☐ 410 ANTITRUST
- ☐ 850 SECURITIES / COMMODITIES / EXCHANGE

OTHER STATUTES - "0" MONTHS DISCOVERY TRACK
- ☐ 896 ARBITRATION (Confirm / Vacate / Order / Modify)

*** PLEASE NOTE DISCOVERY TRACK FOR EACH CASE TYPE. SEE LOCAL RULE 26.3**

VII. REQUESTED IN COMPLAINT:

☑ CHECK IF CLASS ACTION UNDER F.R.Civ.P. 23 DEMAND $ in excess of $5,000,000

JURY DEMAND ☑ YES ☐ NO (CHECK YES ONLY IF DEMANDED IN COMPLAINT)

VIII. RELATED/REFILED CASE(S) IF ANY

JUDGE_____ DOCKET NO._____

CIVIL CASES ARE DEEMED RELATED IF THE PENDING CASE INVOLVES: (CHECK APPROPRIATE BOX)
- ☐ 1. PROPERTY INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.
- ☐ 2. SAME ISSUE OF FACT OR ARISES OUT OF THE SAME EVENT OR TRANSACTION INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.
- ☐ 3. VALIDITY OR INFRINGEMENT OF THE SAME PATENT, COPYRIGHT OR TRADEMARK INCLUDED IN AN EARLIER NUMBERED PENDING SUIT.
- ☐ 4. APPEALS ARISING OUT OF THE SAME BANKRUPTCY CASE AND ANY CASE RELATED THERETO WHICH HAVE BEEN DECIDED BY THE SAME BANKRUPTCY JUDGE.
- ☐ 5. REPETITIVE CASES FILED BY PRO SE LITIGANTS.
- ☐ 6. COMPANION OR RELATED CASE TO CASE(S) BEING SIMULTANEOUSLY FILED (INCLUDE ABBREVIATED STYLE OF OTHER CASE(S)):

☐ 7. EITHER SAME OR ALL OF THE PARTIES AND ISSUES IN THIS CASE WERE PREVIOUSLY INVOLVED IN CASE NO. _____, WHICH WAS DISMISSED. This case ☐ IS ☐ IS NOT (check one box) SUBSTANTIALLY THE SAME CASE.

SIGNATURE OF ATTORNEY OF RECORD

12/14/23

DATE