Exhibit B

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

LAMONT BRACY, *on behalf of himself and all others similarly situated,*	)	
Plaintiffs,	)	Case No. 1:23-cv-05743-TWT
v.	)	
AMERICOLD LOGISTICS LLC,	)	**JURY TRIAL DEMANDED**
Defendant.	)	

CONSOLIDATED CLASS ACTION COMPLAINT

Lamont Bracy, Timothy Chark, Jalisa Samuels, Sean Sheffler, Branden Turner, Brandice Turner, Joseph Vincent ("Plaintiffs") bring this Class Action Complaint against Americold Logistics LLC ("Defendant" or "Americold"), on behalf of themselves and all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and counsels' investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard Personally Identifiable Information ("PII) belonging to Plaintiffs and Class Members including, but not limited to full names, Social

Security numbers, addresses, driver's license numbers, state identification numbers, passport numbers, financial account information (such as bank account and credit card numbers) and employment-related health insurance and medical information (collectively "Private Information").

2. Defendant is an international cold storage, warehousing and logistics limited liability company headquartered in Atlanta, Georgia that provides "technology-based engineered solutions for the temperature-controlled supply chain industry."[1]

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

4. Plaintiffs seek to hold Defendant responsible for the harms it caused and will continue to cause Plaintiffs and over 129,600 other similarly situated persons[2] 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

[1] https://www.americold.com/

[2] 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 Apr. 1, 2024).

highly sensitive Private Information belonging to Plaintiffs and Class Members which was being kept unprotected (the "Data Breach").

5. The Cactus cybercriminal ransomware gang claimed that it accessed and exfiltrated Plaintiffs' and Class Members' Private Information.[3]

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.[4]

[3] https://www.bleepingcomputer.com/news/security/cold-storage-giant-americold-discloses-data-breach-after-april-malware-attack/ (last visited Apr. 1, 2024).

[4] *Id.*

7. Plaintiffs seek to hold Defendant responsible for not maintaining the Private Information 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").[5]

9. Despite knowing that Private Information stolen in the Data Breach would be used for harm, Defendant did not begin notifying victims, like Plaintiffs, or state Attorneys General of the Data Breach until December 8, 2023, over seven months later -- long after Defendant understood the risk that Plaintiffs 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, Plaintiffs' and Class Members' Private Information was likely disseminated on the Dark Web. As a result of this delayed response, Plaintiffs and Class Members were unaware that their Private Information had been compromised, and that Plaintiffs 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

[5] Americold – CA Individual Notice Letters – 12.8.23.pdf

their account and how victims could 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 Plaintiffs' and Class Members' Private Information remains in the possession of criminals.

11. By acquiring, utilizing, and benefiting from Plaintiffs' and Class Members' Private Information for its business and employment purposes, Defendant owed or otherwise assumed common law, contractual, and statutory duties that extended to Plaintiffs and Class Members. These duties required Defendant to design and implement adequate data security systems to protect Plaintiffs' and Class Members' Private Information in its possession and to keep Plaintiffs' and Class Members' Private Information 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 Plaintiffs' and Class Members' Private Information from a foreseeable cyberattack on its systems that resulted in the unauthorized access and theft of Plaintiffs' and Class Members' Private Information.

13. Currently, the full extent of the types of Private Information, the scope of the Data 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 Plaintiffs and Class Members by intentionally, willfully, recklessly, and/or negligently failing to take and implement adequate and reasonable measures to ensure that the Private Information of Plaintiffs 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 Plaintiffs' and Class Members' Private Information was compromised through unauthorized 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 Plaintiffs and Class Members of Defendant's inadequate data security practices; (6) failing to encrypt or adequately

encrypt the Private Information; (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 cyberattack; 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 Private Information involved, Defendant's admission that the Private Information was accessed, and the claims by a criminal ransomware gang that it was responsible for the Data Breach, it can be concluded that the unauthorized criminal third party was able to successfully target Plaintiffs' and Class Members' Private Information, infiltrate and gain access to Defendant's network, and exfiltrate Plaintiffs' and Class Members' Private Information, 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 Private Information for use in fraud and identity theft.

17. As a result of Defendant's failures and the Data Breach, Plaintiffs' 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, Plaintiffs and Class Members must now closely monitor their financial accounts to guard against future identity theft and fraud. Plaintiffs 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. Plaintiffs 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 Private Information; (h) invasions of their privacy; and/or (i) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect it.

20. Plaintiffs bring this action on behalf of all persons whose Private Information was compromised in the Data Breach due to Defendant's failure to adequately protect Plaintiffs' and Class Members' Private Information. Accordingly, Plaintiffs bring this action against Defendant seeking redress for its unlawful conduct and assert claims on behalf of the Class for Negligence; Negligence *Per Se*; Breach of Implied Contract; Unjust Enrichment; violations of O.C.G.A. § 13-6-11; violations of the Georgia Uniform Deceptive Trade Practices Act, O.C.G.A. §§ 13-1-370, *et seq.*; and declaratory judgment under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq*.

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 and intends to remain domiciled in Alabama.

22. Plaintiff Timothy Chark is an adult individual and, at all relevant times herein, a resident and citizen of the state of Iowa, residing in Sioux City, Iowa, in Woodbury County and intends to remain domiciled in Iowa.

23. Plaintiff Jalisa Samuels is an adult individual and, at all relevant times herein, a resident and citizen of the state of Georgia, residing in Lilburn, Georgia, in Gwinnett County and intends to remain domiciled in Georgia.

24. Plaintiff Sean Sheffler is an adult individual and, at all relevant times herein, a resident and citizen of the state of Ohio, residing in Defiance County, Ohio, and intends to remain domiciled in Ohio.

25. Plaintiff Branden Turner is adult individual and, at all relevant times herein, a resident and citizen of the state of Georgia, residing in Powder Springs, Georgia, in Cobb County and intends to remain domiciled in Georgia.

26. Plaintiff Brandice Turner is adult individual and, at all relevant times herein, a resident and citizen of the state of Georgia, residing in Powder Springs, Georgia, in Cobb County and intends to remain domiciled in Georgia.

27. Plaintiff Joseph Vincent is an adult individual and, at all relevant times herein, a resident and citizen of the state of Georgia, residing in Hampton, Georgia, in Henry County and intends to remain domiciled in Georgia.

28. 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, Georgia 30046-4805.

29. According to Florida Secretary of State business filings for Americold Logistics, LLC, Defendant as an LLC, has several members/managers including Art Al Holding, LLC, 10 Glenlake Parkway NE, 600 South Tower, Atlanta, Georgia 30328[6] and Nathan Hale Harwell, 10 Glenlake Parkway NE, 600 South Tower, Atlanta, Georgia 30328.[7]

30. There may be other members/managers 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 Plaintiffs.

JURISDICTION AND VENUE

31. 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 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, is a citizen of a state different from Defendant.

---

[6] https://search.sunbiz.org/Inquiry/CorporationSearch/GetDocument?aggregateId=forl-m99000000256-daebcb0a-cf29-4933-95df-5ceda3683443&transactionId=m99000000256-6c601144-22f6-4da9-b64e-9ee05c5cefbd&formatType=PDF (last visited Apr. 5, 2024).

[7] https://search.sunbiz.org/Inquiry/CorporationSearch/GetDocument?aggregateId=forl-m99000000256-daebcb0a-cf29-4933-95df-ceda3683443&transactionId=m99000000256-007cd6c0-0d29-4498-bbcf-b3bc1d6073ef&formatType=PDF (last visited Apr. 5, 2024).

32. 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 Plaintiffs' claims occurred in and emanated from this District.

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

FACTUAL ALLEGATIONS

Defendant's Business

34. Defendant Americold is a "global leader in temperature-controlled warehousing and logistics, with the largest network in the word."[8] 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.

35. 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.

[8] https://www.americold.com/wp-content/uploads/sites/2/2020/07/Americold-Privacy-Notice-Jan-29-2020-v0.12.pdf (last visited April 5, 2024).

36. To provide these services, and in the ordinary course of Defendant's business, Defendant acquires, possesses, analyzes, and otherwise utilizes Plaintiffs' and putative Class Members' Private Information.

37. Defendant's 2020 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."[9]

38. Defendant's 2020 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."[10]

39. Defendant's website also contains a 2021 Privacy Notice that states it applies to "applicants for employment" and provides that Defendant "collect[s] or

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

[10] *Id*.

obtain[s] Personal Data about you … when you submit a job application."[11]

40. Under "Data security," Defendant's 2021 Privacy Notice states that Defendant "implement[s] appropriate technical and organizational security measures to protect your Personal Data."[12]

41. Under "Data security," Defendant's 2021 Privacy Notice states that Defendant "ha[s] implemented appropriate technical and organizational security measures designed to protect your Personal Data against accidental or unlawful destruction, loss, unauthorized disclosure, unauthorized access, and other unlawful or unauthorized forms of Processing, in accordance with applicable law."[13]

Defendant Acquires, Collects, and Stores the Private Information of Plaintiffs and Class Members

42. In the ordinary course of its business and for employment purposes, Americold maintains the Private Information 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.

---

[11] https://www.americold.com/wp-content/uploads/sites/2/2021/08/Americold-Privacy-Notice_21-08-05.pdf (last visited April 5, 2024).

[12] *Id.*

[13] *Id.*

43. As a condition of employment with Americold, Defendant requires that its employees entrust it with highly sensitive personal information. In the ordinary course of employment with Americold, Plaintiffs and Class Members were required to provide their Private Information to Defendant.

44. Additionally, Defendant may receive Private Information from other individuals and/or organizations including Plaintiffs' and Class Members' employers, insurance carriers, and in connection with enrollment in employee insurance and retirement benefit plans.

45. 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 Private Information, inform consumers and employees of its legal duties and comply with all federal and state laws protecting consumer and employee Private Information; only use and release Private Information for business purposes, and, provide adequate notice to individuals if their Private Information is disclosed without authorization.

46. At every step, Defendant acquires and maintains sensitive Private Information and has a duty to protect that Private Information from unauthorized access.

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

48. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information.

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

The Cyberattack and Data Breach

50. Beginning on or around December 8, 2023, Defendant issued Notice Letters to Plaintiffs and Class Members. In total, at least 129,600 individuals were impacted by the Data Breach.[14]

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

[14] 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 Apr. 1, 2024).

deployment of malware on certain parts of its computer systems.[15]

52. Americold stated that it 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.[16]

53. 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.[17]

54. Plaintiffs' and Class Members' Private Information was exfiltrated and stolen in the attack.

55. Furthermore, the investigation determined that the accessed systems contained Plaintiffs' and Class Members' Private Information. This Private Information was accessible, unencrypted, unprotected, and vulnerable to acquisition and/or exfiltration by the unauthorized actor.

56. The Private Information 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

[15] *See* Notice Letter.

[16] *Id.*

[17] *Id.*

information, health insurance information, and medical information.[18]

57. While Americold stated in the Notice Letter that the unusual activity was discovered on April 26, 2023, Americold did not begin notifying victims until December 8, 2023 – over *seven months* after Americold discovered the Data Breach.[19]

58. Defendant had obligations created by contract, industry standards, common law, and its own promises and representations to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

59. Plaintiffs and Class Members provided their Private Information 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.

60. 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.

[18] *Id.*

[19] *Id.*

61. 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."[20]

62. Americold has offered abbreviated, non-automatic credit monitoring services to victims thereby identifying the harm posed to Plaintiffs 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 immutable Private Information that cannot be changed, such as Social Security numbers.

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

64. As a result of the Data Breach, Plaintiffs and over 129,600 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.

[20] *Id.*

65. Defendant waited more than *seven months* to disclose the Data Breach to Plaintiffs and Class Members. As a result of this delay, Plaintiffs and Class Members had no idea their Private Health Information 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.

66. 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 Private Information.

67. This Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the Private Information of Plaintiffs and Class Members.

68. 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' Private Information 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' and employees' Private Information.

69. Plaintiffs and Class Members directly or indirectly entrusted Defendant

with sensitive and confidential information, including their Private Information which includes information that is immutable and can be used to commit myriad financial crimes.

70. Plaintiffs and Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use their Private Information for authorized purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand Defendant safeguard their Private Information.

71. Plaintiffs' and Class Members' unencrypted Private Information will logically end up for sale on the dark web as that is the *modus operandi* of the Cactus cybercriminal ransomware gang. Indeed, the Cactus cybercriminal ransomware gang, the hackers claiming to be responsible for infiltrating Defendant's inadequately protected computer network, posted on the internet that Americold information would be coming soon.

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

73. Defendant did not use reasonable security procedures and practices

appropriate to the nature of the sensitive, unencrypted information they were maintaining for Plaintiffs and Class Members, causing the exposure of Plaintiffs' and Class Members' Private Information.

The Data Breach Was Foreseeable

74. 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 a prior data breach in 2020 where threat actors gained access to its network.[21]

75. The repeated breach of Americold's systems evinces its flawed data security and its continuous disregard of its obligations to protect Private Information from exposure, compromise, and/or exfiltration by cybercriminals.

76. The November 2020 breach put, or should have put, Americold on notice that further cyberattacks were imminent.

77. Research has indicated that "[r]epeated attacks are actually the norm, not the exception. Some two-thirds (67%) of companies attacked get attacked again within one year."[22]

78. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in many industries

[21]https://www.sec.gov/ix?doc=/Archives/edgar/data/1455863/000119312520294943/d62059d8k.htm (last visited Apr. 1, 2024).

[22] https://securityintelligence.com/articles/how-do-some-companies-get-compromised-again-and-again/ (last visited Apr. 5, 2024).

preceding the date of the breach.

79. Americold was obligated to perform its business operations in accordance with industry standards that require Americold to exercise reasonable care to implement reasonable data security measures that do not create a foreseeable risk of harm to Plaintiffs and the Class Members. Industry best practices put the onus of adequate cybersecurity on the entity most capable of preventing a Data Breach. In this case, Americold was the only entity responsible for adequately protecting the data that they alone solicited, collected, and stored.

80. The injuries to Plaintiffs and Class Members were reasonably foreseeable to Americold because common law, statutes, and industry standards require Defendant to safeguard and protect its computer systems and employ procedures and controls to ensure that unauthorized third parties did not gain access to Plaintiffs' and the other Class Members' Private Information.

81. In the years immediately preceding the Data Breach, Americold knew or should have known that its computer systems and network were a target for cybersecurity attacks, including attacks involving data theft, because it had itself been breached. As such, Americold's own misconduct created a foreseeable risk of harm to Plaintiffs and Class Members.

82. 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.

83. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[23]

84. 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 targets, so they are aware of, and prepared for, potential attack.[24]

85. This readily available and accessible information confirms that, before 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 of companies such as Americold.

---

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

[24] *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).

86. Given that cybercriminals had successfully breached Americold's systems in the past, Americold was on notice that it would likely be the target of another cyberattack but nevertheless failed to implement adequate data security measures to prevent a second, foreseeable data breach from occurring.

87. Before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' Private Information could be accessed, exfiltrated, and published as the result of a cyberattack.

88. Before 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 Private Information to protect against their publication and misuse in the event of a cyberattack.

Defendant Had a Duty to Protect Plaintiffs' and Class Members' Private Information

89. By undertaking to collect, store, and maintain Plaintiffs' and Class Members' Private Information, and deriving monetary benefit from the same, Americold assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

90. Defendant's failure to adequately secure Plaintiffs' and Class Members' Private Information breaches duties it owes Plaintiffs and Class Members under statutory and common law. Moreover, Plaintiffs and Class Members

surrendered their highly 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.

91. 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).

92. The FTC's publication "Protecting Private Information: A Guide for Business" sets forth fundamental data security principles and practices for businesses to implement and follow as a means to protect sensitive data.[25] Among other things, the guidelines note that businesses should (a) protect the personal customer information that they collect and store; (b) properly dispose of Private Information that is no longer needed; (c) encrypt information stored on their computer networks; (d) understand their network's vulnerabilities; and (e) implement policies to correct security problems. The FTC guidelines further

[25] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business

recommend that businesses use an intrusion detection system, monitor all incoming traffic for unusual activity, monitor for large amounts of data being transmitted from their system, and have a response plan ready in the event of a breach.[26]

93. The FTC recommends that organizations limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[27] This is consistent with guidance provided by the Federal Bureau of Investigation ("FBI").

94. The FTC has brought enforcement actions against businesses for failing to reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[28]

95. In addition to its obligations under federal and state laws, Defendant

---

[26] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business

[27] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

[28] https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement

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

96. Defendant owed a duty to Plaintiffs and Class Members to design, maintain, and test its computer systems, servers, and networks to ensure that the Private Information in its possession was adequately secured and protected.

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

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

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

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

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

102. Defendant owed a duty to Plaintiffs and Class Members to encrypt and/or more reliably encrypt Plaintiffs' and Class Members' Private Information and monitor user behavior and activity in order to identify possible threats.

103. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs 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 Plaintiffs and Class Members as a result of a breach.

104. 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' Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

Cybercriminals Target PII to Carry Out Fraud and Identity Theft

105. 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.[29] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[30] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[31]

106. 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.

107. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to

---

[29] 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 Apr. 5, 2024).

[30] 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 Apr. 5, 2024).

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

credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[32]

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

109. 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.[33]

110. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and

---

[32] 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 Apr. 5, 2024).

[33] *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: https://www.gao.gov/assets/gao-07-737.pdf (last visited Apr. 5, 2024).

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 Plaintiffs and Class Members as a result of a breach.

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

112. Defendant has acknowledged the risk and harm caused to Plaintiffs and Class Members as a result of the Data Breach. Defendant, to date, has offered Plaintiffs and Class Members abbreviated, non-automatic credit monitoring services. The limited credit monitoring is inadequate to protect Plaintiffs and Class Members from the threats they face for the remainder of their lives, particularly in light of the immutable nature of the Private Information at issue here. Moreover, Defendant put the burden squarely on Plaintiffs and Class Members to enroll in the inadequate monitoring services.

Defendant's Actions and Inactions Caused the Data Breach

113. Data disclosures and data breaches are preventable.[34] As Lucy

[34] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

Thompson wrote in the Data Breach and Encryption Handbook, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[35] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised [.]"[36]

114. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[37]

115. Defendant could have prevented this Data Breach by properly securing and encrypting the systems containing the Private Information of Plaintiffs 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.

116. Defendant's negligence in affirmatively mishandling its data security, instituting inaccurate security controls, and improperly maintaining and safeguarding the Private Information of Plaintiffs and Class Members is exacerbated

[35] *Id.* at 17.
[36] *Id.* at 28.
[37] *Id.* (emphasis added).

by its own prior breach, and the repeated warnings and alerts directed to companies like Americold to protect and secure sensitive data they possess.

117. Despite experiencing a previous data breach and the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

118. 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."[38]

119. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once PII like the Private Information here is stolen, fraudulent use of that information and

[38] *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).

damage to victims may continue for their respective lifetimes.

120. 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 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.[39]

121. 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

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

> 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 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….[40]

[40] *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 April 5, 2024).

122. 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;

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].[41]

123. Moreover, given that Defendant was storing the Private Information of Plaintiffs and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

124. Americold affirmatively breached its obligations and duties to Plaintiffs and Class Members and/or was otherwise negligent because it mismanaged its data security systems and policies and failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of Plaintiffs and Class Members.

125. 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 Plaintiffs' and Class Members' Private Information.

126. Because Defendant failed to properly protect and safeguard Plaintiffs' and Class Members' Private Information, an unauthorized third party accessed

[41] *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 Apr. 5, 2024).

Defendant's network, and accessed Defendant's database and system configuration files and exfiltrated that data.

127. This Data Breach would not have occurred, and Plaintiffs' and Class Members' Private Information would not be in the hands of criminals, but for Americold's mishandling of its data security.

Defendant Failed to Comply with Industry Standards

128. 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 Private Information which they collect and maintain.

129. 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; requiring 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.

130. 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.

131. 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.

132. 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.

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

Defendant's Negligent Acts and Breaches

134. Defendant participated in and controlled the process of gathering the Private Information from Plaintiffs and Class Members.

135. Defendant therefore assumed and otherwise owed duties and obligations to Plaintiffs 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

Plaintiffs and Class Members and/or was otherwise negligent because it failed to properly implement data security systems and policies that would adequately safeguard Plaintiffs' and Class Members' Private Information. 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 Plaintiffs' and Class Members' Private Information;

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. Failing to comply with its own Privacy Policies;

l. Failing to notify Plaintiffs and Class Members promptly after discovering the Data Breach, and instead waiting over seven months before providing notice of the Data Breach;

m. Otherwise negligently and unlawfully failing to safeguard Plaintiffs' and Class Members' Private Information provided to Defendant, which in turn allowed cyberthieves to access its computer systems and exfiltrate Private Information.

COMMON INJURIES & DAMAGES

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

137. Due to the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs 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 Private Information; and (i) the continued risk to their Private Information, 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 Plaintiffs' and Class Members' Private Information.

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

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

139. 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.

140. 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.

141. The Dark Web is an unindexed layer of the internet that requires special software or authentication to access.[42] 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.[43] This prevents Dark Web marketplaces from being easily monitored by authorities or accessed by those not in the know.

142. 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.[44] The digital character of Private Information

[42]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 Apr. 5, 2024).

[43] *Id.*

[44] *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 Apr. 5, 2024).

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.[45] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[46]

143. 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 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

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

[46] *Id.*

can cause a lot of problems.[47]

> 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.

144. 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."[48]

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

---

[47] 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).

[48] 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).

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.[49]

146. 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.[50]

147. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[51] Defendant did not rapidly report to Plaintiffs and Class Members that their PII had been stolen.

148. 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.

149. 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

[49] *Identity Theft and Your Social Security Number*, Social Security Administration, 1 (2021), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Apr. 5, 2024).

[50] *See 2019 Internet Crime Report*, FBI (Feb. 11, 2020), https://www.fbi.gov/news/stories /2019-internet-crime-report-released-021120 (last visited Apr. 5, 2024).

[51] *Id.*

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.

150. 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, Plaintiffs and Class Members will need to remain vigilant against unauthorized data use for years or even decades to come.

151. The 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."[52]

152. 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

[52] 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).

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.[53]

153. According to the FTC, unauthorized disclosures of Private Information 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 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.[54]

154. Defendant's failure to properly notify Plaintiffs and Class Members of the Data Breach exacerbated Plaintiffs' and Class Members' injury by depriving

[53] *See generally* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Apr. 5, 2024).

[54] *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 Apr. 4, 2024).

them of the earliest ability to take appropriate measures to protect their Private Information and take other necessary steps to mitigate the harm caused by the Data Breach.

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

155. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft 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.

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

157. Plaintiffs 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.

158. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[55]

159. Plaintiffs' 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 credit, and correcting their credit reports.[56]

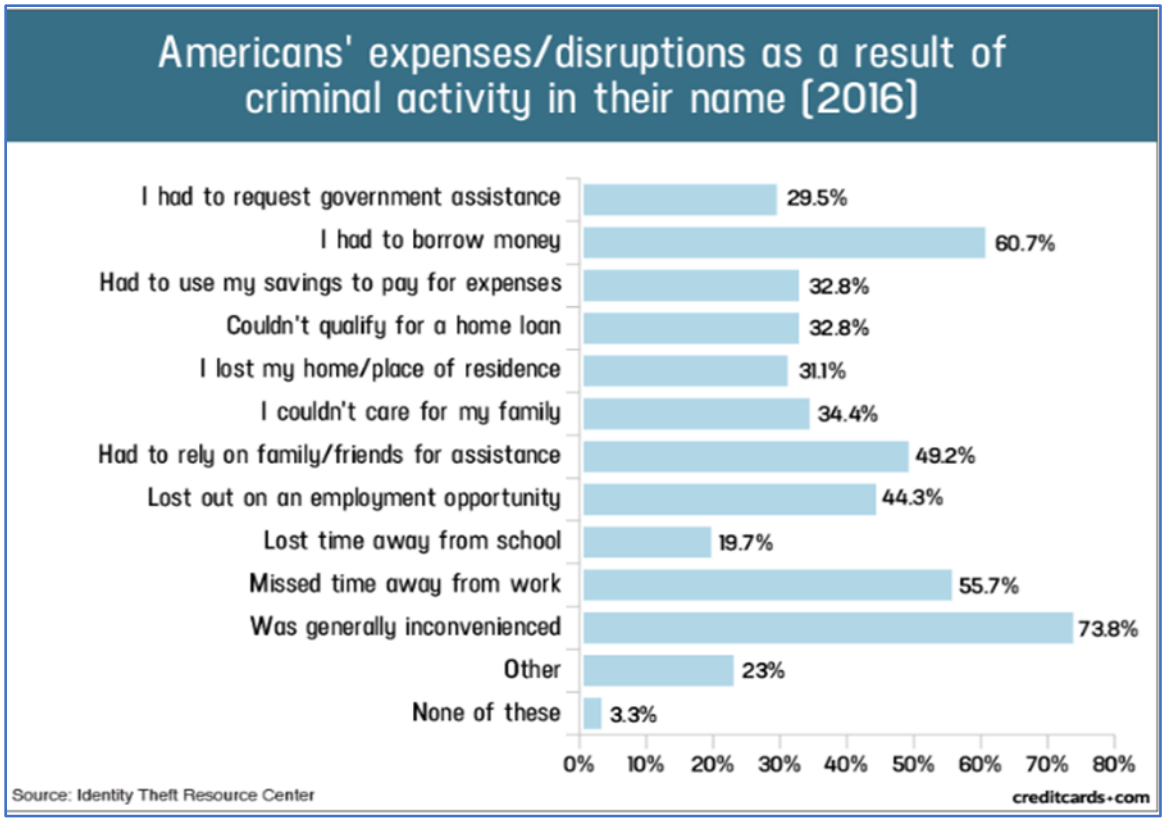
160. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[57]

---

[55] *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).

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

[57] "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).



161. 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 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.[58]

[58] *See* Federal Trade Commission, IdentityTheft.gov, https://www.identitytheft.gov/Steps (last visited Apr. 5, 2024).

Diminution of Value of the Plaintiffs' and Class Members' Private Information

162. Private Information is a valuable property right.[59] 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 Private Information has considerable market value.

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

164. Private Information can sell for as much as $363 per record according to the Infosec Institute.[60]

165. Medical information is especially valuable to identity thieves. Cybersecurity firm Trustwave calculated the black-market value of medical records

[59] *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).

[60] *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 Apr. 5, 2024).

at $250 each.[61]

166. An active and robust legitimate marketplace for Plaintiffs' and Class Members' Private Information exists. In 2019, the data brokering industry was worth roughly $200 billion.[62] 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.[63, 64] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[65]

167. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished in its value by its unauthorized and potential release onto the Dark Web, where it may soon be available and holds significant

[61] 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 Apr. 5, 2024).

[62] 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 Apr. 5, 2024).

[63] https://datacoup.com/ (last visited Apr. 5, 2024).

[64] https://digi.me/questions/what-is-a-digi-me-personal-data-vault (last visited Apr. 5, 2024).

[65] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Apr. 5, 2024).

value for the threat actors.

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

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

169. The abbreviated, limited, and non-automatic credit monitoring offered to Plaintiffs and Class Members whose Private Information 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 Plaintiffs and Class Members by requiring them to independently sign up for that service, as opposed to automatically enrolling all victims of this Data Breach.

170. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information, 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 Private Information for identity theft crimes – e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

171. 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 Private Information is stolen and when it is used.

172. 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.

173. 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.[66] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

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

175. The retail cost of credit monitoring and identity theft monitoring can

[66] *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 Apr. 5, 2024).

cost around $200 a year, or more, per Class Member. This is a reasonable and necessary cost to protect Plaintiffs and 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 Plaintiffs and Class Members would not need to bear, but for Defendant's failure to safeguard their Private Information.

Injunctive Relief Is Necessary to Protect against Future Data Breaches

176. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, 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 Private Information is not accessible online and that access to such data is password protected.

PLAINTIFFS' EXPERIENCES

Lamont Bracy - Alabama

177. At the time of the Data Breach, Defendant retained Plaintiff Bracy's Private Information in its system.

178. Plaintiff Bracy was required to provide his Private Information to Americold when applying for employment and he entrusted Americold with his Private Information. When providing and entrusting Americold with his Private Information, Plaintiff Bracy reasonably expected that his Private Information would

remain safe and not be accessed by unauthorized third parties.

179. Plaintiff Bracy only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic, industry standard data security measures, such as those set forth herein, to protect it from unauthorized access.

180. Plaintiff Bracy received the Notice Letter, by U.S. mail, directly from Defendant, dated December 8, 2023. According to the Notice Letter, Americold stated that an unauthorized party was able to improperly access and remove "some data" from the network. This data included Plaintiff's Private Information, which may have included his "name, address, Social Security number, driver's license/ state ID number, passport number, financial account information . . . employment-related health insurance and medical information."

181. As a result of the Data Breach, Plaintiff Bracy spent time dealing with the consequences of the Data Breach, which includes 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.

182. Plaintiff Bracy is a cautious person and is therefore very careful about sharing his sensitive Private Information. As a result, he has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Bracy stores any documents containing his Private Information 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.

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

184. Plaintiff Bracy suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that Plaintiff Bracy entrusted to Defendant for the purpose of his employment, which was compromised in and as a result of the Data Breach.

185. 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 Private Information being placed in the hands of criminals.

186. 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 Private Information 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 Private Information from the cyber-criminals.

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

188. 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 Private Information, the damages articulated more specifically above are far from the full extent of the harm thereto.

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

190. Plaintiff Bracy suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with

attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

Branden Turner – Georgia

191. Plaintiff Branden Turner is a current employee at Americold.

192. As a condition of obtaining employment at Americold, Plaintiff Branden Turner was required to supply Defendant with his Private Information, including, but not limited to his name, address, and Social Security number. He entrusted Americold with his Private Information. When providing and entrusting Americold with his Private Information, Plaintiff Turner reasonably expected that his Private Information would remain safe and not be accessed by unauthorized third parties.

193. Plaintiff Turner only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic, industry standard data security measures, such as those set forth herein, to protect it from

unauthorized access.

194. At the time of the Data Breach—on or about April 26, 2023—Americold retained Plaintiff Turner's Private Information in its system.

195. Plaintiff Turner is very careful about sharing his sensitive Private Information. Mr. Turner stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

196. Plaintiff Turner received the Notice Letter, by U.S. mail, directly from Defendant, dated December 8, 2023. According to the Notice Letter, Americold stated that an unauthorized party was able to improperly access and remove "some data" from the network. This data included Plaintiff Turner's Private Information, which may have included his "name, address, Social Security number, driver's license/ state ID number, passport number, financial account information . . . employment-related health insurance and medical information."

197. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructed Plaintiff Turner 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 ensure that all activity is valid[,]"[67] Plaintiff Turner made reasonable efforts to mitigate the impact of the Data

[67] Notice Letter.

Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach.

198. After receiving the Notice Letter and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Turner has spent significant time thus far dealing with the Data Breach, including his vacation time for which he was uncompensated for—valuable time Plaintiff Turner otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

199. Plaintiff Turner further suffered actual injury in the form of his Private Information being disseminated on the Dark Web, according to Experian, which, upon information and belief, was caused by the Data Breach.

200. Plaintiff Turner also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

201. Plaintiff Turner suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that Plaintiff Turner entrusted to Defendant for the purpose of his employment, which was compromised in and as a result of the Data Breach.

202. The Data Breach has caused Plaintiff Turner to suffer fear, anxiety, and stress, which has been compounded by the fact that Americold has still not fully

informed him of key details about the Data Breach's occurrence.

203. As a result of the Data Breach, Plaintiff Turner anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Turner is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

204. Plaintiff Turner has a continuing interest in ensuring that his Private Information, which, upon information and belief, remain backed up in Defendant's possession, is protected and safeguarded from future breaches.

205. Plaintiff Turner suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to

undertake appropriate and adequate measures to protect the Private Information.

Brandice Turner – Georgia

206. Plaintiff Brandice Turner receives employee benefits at Americold through her father's (Plaintiff Branden Turner) employment at Americold.

207. As a condition of obtaining employee benefits at Americold, she was required to supply Defendant with her Private Information, and she entrusted Americold with her Private Information. When providing and entrusting Americold with her Private Information, Plaintiff Turner reasonably expected that her Private Information would remain safe and not be accessed by unauthorized third parties.

208. Plaintiff Turner only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic, industry standard data security measures, such as those set forth herein, to protect it from unauthorized access.

209. At the time of the Data Breach—on or about April 26, 2023—Americold retained Plaintiff's Private Information in its system.

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

211. Plaintiff Turner received the Notice Letter, by U.S. mail, directly from

Defendant, dated December 8, 2023. According to the Notice Letter, Americold stated that an unauthorized party was able to improperly access and remove "some data" from the network. This data included Plaintiff Turner's Private Information, which may have included her "name, address, Social Security number, driver's license/ state ID number, passport number, financial account information . . . employment-related health insurance and medical information."

212. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructed Plaintiff Turner 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 ensure that all activity is valid[,]"[68] Plaintiff Turner made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, changing passwords and resecuring her own computer network, and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Turner has spent significant time thus far dealing with the Data Breach—valuable time Plaintiff Turner otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

213. Plaintiff Turner suffered actual injury in the form of experiencing an

[68] Notice Letter.

increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

214. Plaintiff Turner suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff Turner entrusted to Defendant for the purpose of her employment, which was compromised in and as a result of the Data Breach.

215. The Data Breach has caused Plaintiff Turner to suffer fear, anxiety, and stress, which has been compounded by the fact that Americold has still not fully informed her of key details about the Data Breach's occurrence.

216. As a result of the Data Breach, Plaintiff Turner anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Turner is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

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

218. Plaintiff Turner suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished

value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

Jalisa Samuels - Georgia

219. At the time of the Data Breach, Defendant retained Plaintiff Samuels' Private Information in its system.

220. Plaintiff Samuels was required to provide her Private Information to Americold when applying for employment, and she entrusted Americold with her Private Information. When providing and entrusting Americold with her Private Information, Plaintiff Samuels reasonably expected that her Private Information would remain safe and not be accessed by unauthorized third parties.

221. Plaintiff Samuels only allowed Defendant to maintain, store, and use her Private Information because she believed that Defendant would use basic, industry standard data security measures, such as those set forth herein, to protect it

from unauthorized access.

222. As a condition of obtaining employee benefits at Americold, she was required to supply Defendant with her Private Information, including, but not limited to her name, address, and Social Security number.

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

224. Plaintiff Samuels received the Notice Letter, by U.S. mail, directly from Defendant, dated December 8, 2023. According to the Notice Letter, Americold stated that an unauthorized party was able to improperly access and remove "some data" from the network. This data included Plaintiff's Private Information, which may have included her "name, address, Social Security number, driver's license/ state ID number, passport number, financial account information . . . employment-related health insurance and medical information."

225. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructed Plaintiff 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 ensure that all activity is valid[,]"[69] Plaintiff Samuels made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, changing passwords and resecuring her own computer network, placing a freeze on her credit, and monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Samuels has spent significant time thus far dealing with the Data Breach—valuable time Plaintiff Samuels otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

226. Plaintiff Samuels suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

227. Plaintiff Samuels suffered actual injury in the form of damages to and diminution in the value of her Private Information—a form of intangible property that Plaintiff Samels entrusted to Defendant for the purpose of her employment, which was compromised in and as a result of the Data Breach.

228. Plaintiff Samuels was notified by Experian that her Private Information has been found on the Dark Web. Plaintiff Samuels had not received notifications

[69] Notice Letter.

that her information was on the Dark Web before the Americold Data Breach. Plaintiff purchased Dark Web monitoring as a result. Plaintiff Samuels pays $30 per month for the Dark Web monitoring through Experian. The Data Breach has caused Plaintiff Samuels to suffer fear, anxiety, and stress, which has been compounded by the fact that Americold has still not fully informed her of key details about the Data Breach's occurrence.

229. As a result of the Data Breach, Plaintiff Samuels anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Samuels is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

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

231. Plaintiff Samuels suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the

actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

Timothy Chark - Iowa

232. As a condition of obtaining employment at Americold, Plaintiff Chark was required to supply Defendant with his Private Information. He entrusted Americold with his Private Information. When providing and entrusting Americold with his Private Information, Plaintiff Chark reasonably expected that his Private Information would remain safe and not be accessed by unauthorized third parties.

233. Plaintiff Chark only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic, industry standard data security measures, such as those set forth herein, to protect it from unauthorized access.

234. Plaintiff Chark is very careful about sharing his Private Information. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Chark stores any documents containing his sensitive Private Information in a safe and secure location or destroys

the documents.

235. At the time of the Data Breach—on or about April 26, 2023—Americold retained Plaintiff's Private Information in its system.

236. Plaintiff Chark received the Notice Letter, by U.S. mail, directly from Defendant, dated December 8, 2023. According to the Notice Letter, Americold stated that an unauthorized party was able to improperly access and remove "some data" from the network. This data included Plaintiff's Private Information, which may have included his "name, address, Social Security number, driver's license/ state ID number, passport number, financial account information . . . employment-related health insurance and medical information."

237. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructed Plaintiff 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 ensure that all activity is valid[,]"[70] Plaintiff Chark made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, changing passwords and resecuring his own computer network, and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Chark has spent significant time

[70] Notice Letter.

thus far dealing with the Data Breach–valuable time Plaintiff Chark otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

238. The Data Breach has caused Plaintiff Chark to suffer fear, anxiety, and stress, which has been compounded by the fact that Americold has still not fully informed her of key details about the Data Breach's occurrence.

239. Plaintiff suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

240. Plaintiff Chark suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that Plaintiff Chark entrusted to Defendant for the purpose of his employment, which was compromised in and as a result of the Data Breach.

241. As a result of the Data Breach, Plaintiff Chark anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Chark is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

242. Plaintiff Chark has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's

possession, is protected and safeguarded from future breaches.

243. Plaintiff Chark suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

Sean Sheffler - Ohio

244. As a condition of employment, Defendant required Plaintiff Sheffler to provide his Private Information to Americold in or around 2019 when applying for employment, and he entrusted Americold with his Private Information. When providing and entrusting Americold with his Private Information, Plaintiff Sheffler reasonably expected that his Private Information would remain safe and not be accessed by unauthorized third parties.

245. Plaintiff Sheffler only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic, industry standard data security measures, such as those set forth herein, to protect it from unauthorized access.

246. Plaintiff Sheffler is very careful about sharing his Private Information. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Sheffler stores any documents containing his sensitive Private Information in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

247. Plaintiff Sheffler received the Notice Letter, by U.S. mail, directly from Defendant, dated December 8, 2023. According to the Notice Letter, an unauthorized party was able to improperly access and remove "some data" from the network. The Notice Letter stated this data may have included Plaintiff's Private Information, including his "name, address, Social Security number, driver's license/ state ID number, passport number, financial account information . . . employment-related health insurance and medical information."

248. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructed Plaintiff 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 ensure that all activity is valid[,]"[71] Plaintiff Sheffler made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, changing passwords and resecuring his own computer network, and monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. Plaintiff Sheffler has spent significant time thus far dealing with the Data Breach–valuable time Plaintiff Sheffler otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

249. Plaintiff Sheffler suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

250. Plaintiff Sheffler suffered actual injury in the form of damages to and diminution in the value of his Private Information—a form of intangible property that Plaintiff Sheffler entrusted to Defendant for the purpose of his employment, which was compromised in and as a result of the Data Breach.

251. The Data Breach has caused Plaintiff Sheffler to suffer fear, anxiety, and stress, which has been compounded by the fact that Americold has still not fully informed him of key details about the Data Breach's occurrence.

[71] Notice Letter.

252. As a result of the Data Breach, Plaintiff Sheffler anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff Sheffler is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

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

254. Plaintiff Sheffler suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

Joseph Vincent – Georgia

255. Plaintiff Joseph Vincent is a former applicant for employment with Defendant.

256. As a condition of applying for a job with Americold, Plaintiff Vincent was required to provide his Private Information to Defendant, including his name, social security number, and full health and financial information.

257. At the time of the Data Breach on April 26, 2023, Defendant retained Plaintiff Vincent's Private Information in its system.

258. Plaintiff Vincent is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Vincent would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

259. Plaintiff Vincent received the Notice Letter, by U.S. mail, directly from Defendant, dated December 8, 2023. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including his name, address, Social Security number, driver's license/state ID number, passport number, financial account information, and employment-related health insurance and medical information.

260. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, Plaintiff Vincent made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, changing passwords and resecuring his own computer network, and contacting companies regarding suspicious activity on his accounts. Plaintiff Vincent has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

261. Plaintiff Vincent further suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breach.

262. The Data Breach has caused Plaintiff Vincent to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

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

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

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

CLASS ALLEGATIONS

266. Plaintiffs bring this nationwide class action on behalf of themselves 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.

267. The nationwide Class that Plaintiffs seek to represent is defined as follows:

> **All United States residents who were sent a Notice Letter by Defendant Americold Logistics LLC on or about December 8, 2023, notifying them that their Private Information was compromised in the Data Breach (the "Nationwide Class").**

268. The Nationwide Class is referred to herein as the "Class."

269. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs asserts claims on behalf of a separate subclass, defined as follows:

> **All job applicants and current or former employees of Defendant Americold Logistics LLC who were sent a Notice Letter by Defendant Americold Logistics LLC on or about December 8, 2023, notifying them that their Private Information was compromised in the Data Breach (the "Subclass").**

270. 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.

271. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

272. 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 Private Information compromised in this Data Breach.[72] The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

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

[72] *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).

individual Class Members. These include:

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

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

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

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

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

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

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

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

i. Whether Defendant adequately addressed and fixed the vulnerabilities

which permitted the Data Breach to occur;

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

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

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

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

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

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

275. 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 Plaintiffs' 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.

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

277. 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.

278. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because 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 Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

279. 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.

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

281. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information 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.

282. Further, Defendant has acted or refused to act on grounds generally applicable to the Class 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.

283. 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 Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiffs and Class

Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

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 Plaintiffs 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 Plaintiffs and Class Members that their Private Information 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 Private Information of Plaintiffs 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
(On Behalf of Plaintiffs and the Nationwide Class)

284. Plaintiffs re-allege and incorporate by reference the allegations contained in Paragraphs 1 through 283 above as if fully set forth herein.

285. Plaintiffs and the Class entrusted Defendant with their Private Information.

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

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

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

289. 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 Private Information of Plaintiffs and the Class in Defendant's possession was adequately secured and protected.

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

291. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiffs and the Class.

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

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

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

295. Plaintiffs and the Class were the foreseeable and probable victims of

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

296. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs 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 Private Information of Plaintiffs and the Class, including basic encryption techniques freely available to Defendant.

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

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

299. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs 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 Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the

fraudulent use of their Private Information by unauthorized third parties.

300. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiffs and the Class.

301. Defendant has admitted that the Private Information of Plaintiffs and the Class was wrongfully accessed and disclosed to unauthorized third persons as a result of the Data Breach.

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

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

304. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the Private Information of Plaintiffs and the Class in the face of increased risk of theft.

305. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of Private Information.

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

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

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

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

310. As a direct and proximate result of Defendant's negligence, Plaintiffs 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 Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information;

(iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the 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 Private Information, 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 Private Information of Plaintiffs 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 Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

311. As a direct and proximate result of Defendant's negligence, Plaintiffs 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.

312. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks

of exposure of their Private Information, 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 Private Information in its continued possession.

313. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages as a result of the Data Breach.

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

COUNT II
NEGLIGENCE PER SE
(On behalf of Plaintiffs and the Nationwide Class)

315. Plaintiffs re-allege and incorporate by reference the allegations contained in Paragraphs 1 through 283 above as if fully set forth herein.

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

317. 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 customers or, in this case, employees' and prospective employees' Private Information.

318. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the Class Members' sensitive Private Information.

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

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

321. Defendant had a duty to Plaintiffs and the Class Members to implement and maintain reasonable security procedures and practices to safeguard their Private Information.

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

323. Defendant's violation of Section 5 of the FTC Act and its failure to comply with applicable laws and regulations constitutes negligence per se.

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

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

326. Had Plaintiffs and Members of the Class known that Defendant did not adequately protect employees' and prospective employees' Private Information, Plaintiffs and the Class would not have entrusted Defendant with their Private

Information.

327. As a direct and proximate result of Defendant's negligence per se, Plaintiffs 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 Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the 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 Private Information, 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 Private Information of Plaintiffs 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 Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

328. As a direct and proximate result of Defendant's negligence *per se*,

Plaintiffs 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.

329. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, 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 Private Information in its continued possession.

330. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages as a result of the Data Breach.

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

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Subclass)

332. Plaintiffs re-allege and incorporate by reference the allegations

contained in Paragraphs 1 through 283 above as if fully set forth herein.

333. Defendant's 2021 Privacy Notice, which applies to "applicants for employment," provides that Defendant "collect[s] or obtain[s] Personal Data about you … when you submit a job application."

334. Under "Data security," Defendant's 2021 Privacy Notice states that Defendant "implement[s] appropriate technical and organizational security measures to protect your Personal Data."

335. Under "Data security," Defendant's 2021 Privacy Notice states that Defendant "ha[s] implemented appropriate technical and organizational security measures designed to protect your Personal Data against accidental or unlawful destruction, loss, unauthorized disclosure, unauthorized access, and other unlawful or unauthorized forms of Processing, in accordance with applicable law."

336. In applying for employment with Defendant, each Plaintiff submitted their Private Information, including their Social Security numbers, to Defendant.

337. The 2021 Privacy Notice confirms that Defendant intended to bind itself to protect the Private Information, including Social Security numbers, that each Plaintiff submitted to Defendant in applying for employment with Defendant.

338. Defendant required Plaintiffs to provide their personal information, including names, Social Security numbers, and dates of birth, and other personal information, as a condition of their employment. Defendant may have also required

Plaintiffs and the Subclass to provide their government issued ID numbers, financial account numbers, credit/debit card numbers, passwords or login credentials, digital signatures, mother's maiden names, birth certificates, biometric information, and medical/health insurance information as a condition of employment.

339. As a condition of their employment with Defendant, Plaintiffs and the Subclass provided their personal and financial information, including but not limited to the personal information of their beneficiaries and dependents. In so doing, Plaintiffs and the Subclass 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 Plaintiffs and the Subclass if their data had been breached and compromised or stolen.

340. Plaintiffs and the Subclass fully performed their obligations under the implied contracts with Defendant.

341. Defendant breached the implied contracts it made with Plaintiffs and the Subclass by failing to implement appropriate technical and organizational security measures designed to protect their Private Information against accidental or unlawful unauthorized disclosure or unauthorized access and otherwise failing to safeguard and protect their personal and financial information, including the personal information of their beneficiaries and dependents, and by failing to provide timely and accurate notice to them that personal and financial information, along

with the personal information of their beneficiaries and dependents, was compromised as a result of the data breach.

342. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Subclass 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.

343. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Subclass are entitled to recover actual, consequential, and nominal damages.

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Subclass)

344. Plaintiffs re-allege and incorporate by reference the allegations contained in Paragraphs 1 through 283 above as if fully set forth herein.

345. Plaintiffs and the Subclass bring this claim in the alternative to their

claim for breach of implied contract above.

346. Plaintiffs and the Subclass conferred a monetary benefit to Defendant in the form of providing their Private Information to Defendant, without which Defendant would be unable to conduct its regular course of business.

347. Defendant knew that Plaintiffs and Subclass Members conferred a monetary benefit to Defendant and it accepted and retained that benefit. Defendant profited from this monetary benefit, as the transmission of Private Information to Defendant from Plaintiffs and Subclass Members is an integral part of Defendant's business. Without collecting and maintaining Plaintiffs' and Subclass Members' Private Information, Defendant would not be able to perform its services.

348. Defendant was supposed to use some of the monetary benefit provided to it by Plaintiffs and Subclass Members to secure the Private Information belonging to Plaintiffs and Subclass Members by paying for costs of adequate data management and security.

349. Defendant should not be permitted to retain any monetary benefit belonging to Plaintiffs and Subclass Members because Defendant failed to implement necessary security measures to protect the Private Information of Plaintiffs and Subclass Members.

350. Defendant gained access to the Plaintiffs' and Subclass Members' Private Information through inequitable means because Defendant failed to disclose

that it used inadequate security measures.

351. Plaintiffs and Subclass Members were unaware of the inadequate security measures and would not have entrusted their Private Information to Defendant had they known of the inadequate security measures.

352. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Subclass Members' Private Information.

353. Defendant was also enriched from the value of Plaintiffs' and Subclass Members' Private Information. Private Information 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.

354. 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 Plaintiffs and Subclass Members by utilizing cheaper, ineffective security measures. Plaintiffs and Subclass Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

355. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Subclass Members, because Defendant failed to implement appropriate data

management and security measures that are mandated by industry standards.

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

357. If Plaintiffs and Subclass Members knew that Defendant had not secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

358. To the extent that this cause of action is pleaded in the alternative to the others, Plaintiffs and Subclass Members have no adequate remedy at law.

359. As a direct and proximate result of Defendant's conduct, Plaintiffs and Subclass Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual 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 Private Information, which remains in Defendant's possession and is subject to further

unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; 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 Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Subclass Members.

360. As a direct and proximate result of Defendant's conduct, Plaintiffs and Subclass Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and noneconomic losses.

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

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

362. Plaintiffs re-allege and incorporate by reference the allegations contained in Paragraphs 1 through 283 above as if fully set forth herein.

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

364. 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 Private Information.

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

366. 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.

367. 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.

368. 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 Plaintiffs 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).

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

370. Despite that knowledge, Defendant abdicated its duty to protect the Private Information it required Plaintiffs and the Class to provide and that it stored.

371. As a direct and proximate result of Defendant's actions, Plaintiffs' and the Class Members' Private Information 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 Private Information unsecured. Had Defendant adopted reasonable data security measures, it could have prevented the Data Breach.

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

373. Plaintiffs 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.*
(On Behalf of Plaintiffs and the Nationwide Class)

374. Plaintiffs re-allege and incorporate by reference the allegations contained in Paragraphs 1 through 283 above as if fully set forth herein.

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

376. 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.

377. 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 Plaintiffs' and Class Members' Private Information, 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 Plaintiffs' and Class Members' Private Information. Defendant made implied or implicit representations that its data security practices were sufficient to protect Plaintiffs' and Class Members' Private Information. By virtue of accepting Plaintiffs' and Class Members' Private Information, Defendant implicitly represented that its data security processes were sufficient to safeguard the Private Information;

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 Plaintiffs' and Class Members' Private Information, 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 Plaintiffs' and Class Members' Private Information, 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 Plaintiffs' and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

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

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class Members' Private Information; 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 Plaintiffs' and Class Members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

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

379. 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 Plaintiffs' and Class Members' Private Information.

380. Defendant intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions.

381. Plaintiffs and Class Members relied on Defendant to advise them if their data security and data storage systems were not adequately secure to protect their Private Information.

382. Plaintiffs 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 Plaintiffs and Class Members that their data security and data storage systems were not adequately secure and, thus, were vulnerable to attack.

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

384. Had Defendant disclosed that its data security and data storage systems were not secure, and thus, vulnerable to attack, Plaintiffs and Class Members would not have entrusted Defendant with their Private Information.

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

386. Had Defendant disclosed to Plaintiffs 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 Private Information regarding thousands of persons, including Plaintiffs 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 Private Information, Plaintiffs and the Class acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

387. As a direct and proximate result of Defendant's unfair and deceptive business practices, Plaintiffs 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 Private Information, 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.

388. 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 Plaintiffs' and Class Members' Private Information 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 Private Information entrusted to it. Without adequate improvements, Plaintiffs' and Class Members' Private Information remains at an unreasonable risk of future compromise.

389. Defendant, through its omissions and its Data Breach Notice Letters, continues to represent and imply that its data security measures are adequate to protect Plaintiffs' and Class Members' Private Information. Such continued representations and implications, without disclosure of the full scope of the Data Breach or Defendant's subsequent remedial enhancements, place Plaintiffs and Class Members at a future risk of harm, as Plaintiffs 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 Plaintiffs and Class Members

remain at an unreasonable risk from future cyberattacks.

390. Plaintiffs and the Class are therefore entitled to the injunctive relief sought herein, because, among other things, Defendant continues to retain their Private Information, 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 Private Information of Plaintiffs and Class Members from future cyberattacks without providing any firm details or basis to support these representations.

391. The Georgia UDTPA 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.

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

393. Plaintiffs and Class Members seek all monetary and non-monetary relief allowed by the Georgia UDTPA, including injunctive relief and attorneys' fees.

COUNT VII
DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Nationwide Class)

394. Plaintiffs re-allege and incorporate by reference the allegations contained in Paragraphs 1 through 283 above as if fully set forth herein.

395. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and common law described in this Complaint.

396. Americold owes a duty of care to Plaintiffs and Class Members, which required it to adequately secure Plaintiffs' and Class Members' Private Information.

397. Americold still possesses Private Information regarding Plaintiffs and Class Members.

398. Plaintiffs allege that Americold's data security measures remain

inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

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

a. Americold owes a legal duty to secure its current and former employees' Private Information from unauthorized disclosure and theft;

b. Americold's existing security measures do not comply with its implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect current and former employees' Private Information; and,

c. Americold continues to breach this legal duty by failing to employ reasonable measures to secure current and former employees' Private Information.

400. This Court should also issue corresponding prospective injunctive relief Requiring Americold to employ adequate security protocols consistent with legal and industry standards to protect current and former employees' Private Information, including the following:

a. Order Americold to provide lifetime credit monitoring and identity

theft insurance to Plaintiffs and Class Members; and,

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Americold must implement and maintain reasonable security measures, including, but not limited to:

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

   ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

   iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

   iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Americold's systems;

   v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

vii. routinely and continually purging all former employee data that is no longer necessary in order to adequately conduct its business operations; and

viii. meaningfully educating its current and former employees about the threats they face with regard to the security of their Private Information, as well as the steps Americold's current and former employees should take to protect themselves.

401. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Americold. The risk of another such breach is real, immediate, and substantial. If another breach at Americold occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

402. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Americold if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Americold's compliance with an injunction

requiring reasonable prospective data security measures is relatively minimal, and Americold has a pre-existing legal obligation to employ such measures.

403. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Americold, thus preventing future injury to Plaintiffs and other current and former employees whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, 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 Plaintiffs and their Counsel to represent the Class;

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

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

an order:

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

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

iii. requiring Defendant to delete, destroy, and purge the Private Information of Plaintiffs 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 Plaintiffs and Class Members;

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

v. 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;

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

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

viii. 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;

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

x. 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 Private Information, as well as protecting the Private Information of Plaintiffs and Class Members;

xi. 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;

xii. 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;

xiii. 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;

xiv. 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;

xv. 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 Plaintiffs and the putative Class Members as to all issues so triable.

Date: April 5, 2024

Respectfully Submitted,

/s/ Terence R. Coates
Terence R. Coates*
Justin C. Walker*
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

MaryBeth V. Gibson
GIBSON CONSUMER LAW GROUP, LLC
Georgia Bar No. 725843
4729 Roswell Road
Suite 208-108
Atlanta, GA 30342
Phone: 678.642.2503
marybeth@gibsonconsumerlawgroup.com

John A. Yanchunis*
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Tel.: (813) 223-5505
jyanchunis@ForThePeople.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 Monroe Street, Suite 2100
Chicago, IL 60606
Phone: 866.252.0878
gklinger@milberg.com

John J. Nelson**
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
280 S. Beverly Drive
Beverly Hills, CA 90212
Telephone: (858) 209-6941
Email: jnelson@milberg.com

Counsel for Plaintiffs and the Putative Class

**admitted pro hac vice*
*** pro hac vice forthcoming*

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.

Dated: April 5, 2024

/s/ Terence R. Coates
Terence R. Coates

CERTIFICATE OF SERVICE

I hereby certify that I have this day filed the within and foregoing CONSOLIDATED CLASS ACTION COMPLAINT upon all parties to this matter by electronically filing a copy of same with the Court's CM/ECF system, which will automatically send an electronic copy to all counsel of record.

Dated this 5th day of April, 2024.

/s/ Terence R. Coates
Terence R. Coates