UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF GEORGIA

JOHN MCNALLY JOYCE NEWMAN, ANDREW SNAITH, PATRICIA KENNEMUR, KELLY COLLINS, DEANA LINDLEY, JOSH STROCK, MOHAMAD RAYCHOUNI, and NATHANIEL SEIBERT, *individually and on behalf of all others similarly situated.* Plaintiffs, v. INFOSYS MCCAMISH SYS., LLC., Defendant.	Case No. 1:24-CV-00995-JPB Judge J.P. Boulee **CONSOLIDATED CLASS ACTION COMPLAINT** JURY TRIAL DEMANDED

Plaintiffs John McNally Joyce Newman, Andrew Snaith, Patricia Kennemur, Kelly Collins, Deana Lindley, Josh Strock, Mohamad Raychouni, and Nathaniel Seibert ("Plaintiffs"), individually and on behalf of all others similarly situated ("Class Members," defined *infra*), allege the following against Defendant InfoSys McCamish Sys., LLC ("IMS," or "Defendant"), based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by Plaintiffs' counsel and review of public documents as to all other matters:

SUMMARY OF THE CASE

1. This class action arises out of the recent preventable cyberattack and

data breach resulting from Defendant's failure to implement reasonable and industry standard data security practices sufficient to safeguard the confidential personal information of Plaintiffs and Class Members.

2. Defendant IMS offers a platform-based insurance process management solutions to over 34 insurance companies[1] (the "IMS Clients"), across a broad array of insurance products, distribution models, and platform deployment options.[2]

3. To provide its services and in the ordinary course of IMS's business, Defendant requires the IMS Clients' customers to provide their personally identifiable information ("PII"), including but not limited to, their names, Social Security numbers, dates of birth, medical treatment/record information, biometric data, email address and passwords, usernames and passwords, driver's license numbers/State ID numbers, financial account information, payment card information, passport numbers, tribal ID numbers and U.S. military ID numbers.[3]

[1] Included in this list of 34 are Oceanview Life and Annuity company, Bank of America, Fidelity Investments Life Insurance, Newport Group, Union Labor Life Insurance, Magnastar Life/M Financial/Prudential, Foresters Financial, Teachers Insurance and Annuity Association of America d/b/a TIAA ("TIAA"), New York Life Insurance Co d/b/a New York Life Group Benefits Solutions ("New York Life"), T.Rowe Price, USAA, Northwestern Mutual, Global Atlantic Financial Group, Continental Casualty Company ("Continental"), and Vanguard, all of whom have customers who were affected by the Data Breach incident in November 2023.

[2] *See* https://www.infosysbpm.com/mccamish/about.html

[3] *See* https://www.maine.gov/cgi-bin/agviewerad/ret?loc=668

4. IMS is a processor and supports corporate and business market operations for certain organizations. IMS collected and stored the sensitive PII of Plaintiffs and Class members in an unencrypted manner and in an internet accessible environment. Between October 29, 2023, and November 2, 2023, cybercriminals deployed ransomware on IMS's inadequately secured systems and accessed and exfiltrated the PII of Plaintiffs and Class Members (the "Data Breach").

5. Although various forms of PII of Plaintiffs and Class Members had been acquired in the Data Breach, IMS inexplicably waited over six months until June 2024 to begin notifying victims of the Data Breach through a notice of data breach letter (the "Notice Letter").

6. Victims of the Data Breach include customers of the IMS Clients for whom IMS provides its platform-based insurance process solutions.

7. IMS's misconduct includes negligently and/or recklessly failing to implement adequate and reasonable data security measures to protect Plaintiffs' and Class Members' PII, including specifically, failing to encrypt or redact PII stored on internet accessible network environment, failing to monitor its systems to detect intrusions and prevent further access, failing to limit remote access to PII to only necessary employees, failing to have in place protocols to timely detect the Data Breach and stop the Data Breach, failing to disclose the material facts that they did not have adequate security practices and employee training in place to safeguard the

PII, and failing to provide timely and adequate notice of the Data Breach.

8. The Data Breach was a direct result of Defendant's conduct and failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect its customers' PII from a foreseeable and preventable cyber-attack.

9. Defendant disregarded the rights of Plaintiffs and Class Members by, inter alia, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' PII; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

10. Plaintiffs' and Class Members' identities are now at risk because of Defendant's negligent conduct because the PII that Defendant collected and maintained is now in the hands of data thieves who target and acquire PII for its use in committing fraud and identity theft.

11. Armed with the PII accessed in the Data Breach, data thieves have already engaged in identity theft and fraud and can in the future commit a variety of crimes including, *e.g.*, opening new fraudulent financial accounts in Class Members'

names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest. This risk will continue for the rest of their lives, as Plaintiffs and Class Members are now forced to deal with the danger of identity thieves possessing and fraudulently using their PII which includes immutable information that cannot be changed, like Social Security numbers.

12. Plaintiffs bring this Class Action on behalf all those similarly situated to address Defendant's negligence and inadequate safeguarding of Class Members' PII that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access by an unknown third party.

13. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was accessed during the Data Breach.

14. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

15. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Plaintiff is a citizen of a state different from Defendant to establish minimal diversity.

16. Under 28 U.S.C. § 1332(d)(10), IMS is a citizen of Georgia because it is a Georgia limited liability company and its principal place of business is in Atlanta, Georgia.

17. Further, upon information and belief, at least one member of Defendant is Infosys BPM Limited, a foreign profit corporation, providing for minimal diversity pursuant to 28 U.S.C. § 1332(d)(2)(C).

18. The Court has personal jurisdiction over IMS because IMS is headquartered in Atlanta, Georgia. IMS also conducts substantial business in Georgia related to Plaintiffs and Class Members and has thereby established minimum contacts with Georgia sufficient to authorize this Court's exercise of jurisdiction over IMS.

19. Venue is proper in this District under 28 U.S.C. §1391(b) because IMS collected and maintained Plaintiffs' and Class Members' PII in this District and a

substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

PARTIES

A. PLAINTIFFS

Plaintiff John McNally

20. Plaintiff John McNally is an adult individual, and at all relevant times herein, a resident and citizen of Georgia.

21. Plaintiff McNally provided his PII to Defendant in order to obtain services from Defendant through his Bank of America account, which was an IMS Client utilizing its platforms. Upon information and belief, Plaintiff McNally's PII was stored and maintained by Defendant IMS.

22. Plaintiff McNally received a Notice Letter from Defendant IMS, dated February 6, 2024, informing him of the Data Breach and the unauthorized exposure of his PII.

Plaintiff Patricia Ann Kennemur

23. Plaintiff Patricia Ann Kennemur is an adult individual and at all relevant times herein, a resident and citizen of Texas.

24. Plaintiff Kennemur, insured by New York Life Group Benefits solutions through her work, provided her PII to them as a condition of receiving

insurance through her employer. Upon information and belief, Plaintiff Kennemur's PII was stored and maintained by Defendant IMS.

25. Plaintiff Kennemur received two Notice Letters from Defendant IMS dated June 27, 2023, and September 5, 2024, informing her of the Data Breach and the unauthorized exposure of her PII.

26. The Notice Letter informed Plaintiff Kennemur that her name, employee ID, personal address, Social Security number, financial account number, and date of birth were compromised in the Data Breach.

Plaintiff Kelly Collins

27. Plaintiff Kelly Collins is an adult individual, and at all relevant times herein, a resident and citizen of Arkansas.

28. Plaintiff Collins provided her PII to Defendant in order to obtain services from Defendant through her Bank of America account, which was an IMS Client utilizing its platforms. Upon information and belief, Plaintiff Collins's PII was stored and maintained by Defendant IMS.

29. Plaintiff Collins received a Notice letter from Defendant IMS in March 2024, informing her of the Data Breach and the unauthorized exposure of her PII.

Plaintiff Deana Lindley

30. Plaintiff Deana Lindley is an adult individual, and at all relevant times herein, a resident and citizen of North Carolina.

31. Plaintiff Lindley, a customer of IMS Client Continental Casualty Company, her long-term care insurance, required her to provide her PII to them as a condition of being insured. Upon information and belief, Plaintiff Lindley's PII was stored and maintained by Defendant IMS.

32. Plaintiff Lindley received a Notice Letter from Defendant IMS, dated June 27, 2024, informing her of the Data Breach and the unauthorized exposure of her PII.

Plaintiff Josh Strock

33. Plaintiff Josh Strock is an adult individual, and at all times herein, a resident and citizen of Georgia.

34. Plaintiff Strock provided his PII to IMS Client New York Life Insurance Co. in order to receive insurance coverage through his benefit package at work. Upon information and belief, Plaintiff Strock's PII was stored and maintained by Defendant IMS.

35. Plaintiff Strock received a Notice Letter from Defendant IMS in November 2023, informing him of the Data Breach and the unauthorized exposure of his PII.

36. The Notice Letter informed Plaintiff Strock that his Name, Date of Birth, Employee ID, Financial Accounts, Personal Address, Social Security

Number, Client Information, and Policy Information were compromised in the Data Breach.

Plaintiff Mohamad Raychouni

37. Plaintiff Mohamad Raychouni is an adult individual, and at all relevant times herein, a resident and citizen of Michigan.

38. Plaintiff Raychouni is unaware how IMS received his PII, however, the Notice Letter he received from IMS states his PII was procured through IMS's relationship with Foresters Financial. Upon information and belief, Plaintiff Raychouni's PII was stored and maintained by Defendant IMS.

39. Plaintiff Raychouni received a Notice Letter from Defendant IMS dated September 26, 2024, informing him of the Data Breach and the unauthorized exposure of his PII.

40. The Notice Letter informed Plaintiff Raychouni that his Name, Financial Account Number, and Social Security Number were compromised in the Data Breach.

Plaintiff Nathaniel Seibert

41. Plaintiff Nathaniel Seibert is an adult individual, and at all relevant times herein, a resident and citizen of Florida.

42. Plaintiff Seibert is unaware how IMS obtained his PII, but the Notice Letters he received from IMS state he was implicated in the Data Breach through

IMS Client New York Life Group Benefit Solutions. Upon information and belief, Plaintiff Seibert's PII was stored and maintained by Defendant IMS.

43. Plaintiff Seibert received several Notice Letters. He received four Notice Letters from Defendant IMS dated September 5, 2024, and an additional letter dated June 27, 2024, informing him of the Data Breach and the unauthorized exposure of his PII.

44. The Notice Letter informed Plaintiff Seibert that his Name, Financial Account Numbers, and Social Security Number were compromised in the Data Breach.

Plaintiff Joyce Newman

45. Plaintiff Joyce Newman is an adult individual, and at all times herein, a resident and citizen of New York.

46. Plaintiff Newman, was a customer of IMS Client TIAA and TIAA Life Insurance, and provided her Personal Information in order to receive coverage. Upon information and belief, Plaintiff Newman's PII was stored and maintained by Defendant IMS.

47. Plaintiff Newman received a Notice Letter from Defendant IMS, dated March 7, 2024, informing her of the Data Breach and the unauthorized exposure of her PII.

48. The Notice Letter informed Plaintiff Newman that "some of your personal information was involved in this incident." The Letter did not provide specific details as to what information was disclosed.

Plaintiff Andrew Snaith

49. Plaintiff Andrew Snaith is an adult individual, and at all times herein, a resident and citizen of Pennsylvania.

50. Plaintiff Snaith, provided his Personal Information to IMS Client New York Life Group Benefits in order to receive benefits through his employer. Upon information and belief, Plaintiff Snaith's PII was stored and maintained by Defendant IMS.

51. Plaintiff Snaith received a Notice Letter from Defendant IMS, dated September , 2024, informing him of the Data Breach and the unauthorized exposure of his PII.

52. The Notice Letter informed Plaintiff Snaith that some of his personal information was involved in the Data breach Incident.

B. DEFENDANT

53. Defendant InfoSys McCamish Systems, LLC, is a Georgia limited liability corporation headquartered at 3225 Cumberland Blvd SE, Suite 700, Atlanta, GA 30339. Upon information and belief, its sole member is Infosys BPM Limited, a foreign corporation.

FACTUAL ALLEGATIONS

A. THE DATA BREACH

54. According to the Notice Letters, on November 2, 2023, IMS "became aware that certain IMS systems were encrypted by ransomware." ("the Data Breach").[4]

55. IMS claims that it launched "an investigation with the assistance of third-party cybersecurity experts" after discovering the Data Breach.[5]

56. IMS notified the Office of the Maine Attorney General that compromised data includes affected persons' full names, Social Security numbers, driver's licenses or other government issued identification numbers, medical treatment/record information, biometric data, email addresses and passwords, usernames and passwords, financial account information, payment card information, passport numbers, tribal identification numbers, U.S. military identification numbers, and Dates of Birth.[6]

57. According to a notice of data breach filed with the Attorney General of Maine, the Data Breach has affected 6,078,263 individuals.[7]

---

[4] *See Data Breach Notifications*, Office of the Maine Attorney General, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/b152fd39-9f84-4ca5-a149-d20b94ed8ef6.html ("Notice Letter").

[5] *Id.*

[6] *Id*.

[7] *See id.*

58. IMS notified the Office of the Maine Attorney General that the Data Breach occurred from October 29, 2023, until November 2, 2023.[8]

59. IMS identified a ransomware gang named LockBit as responsible for the Data Breach.[9]

60. LockBit claimed responsibility for the Data Breach on November 4, 2023.[10]

61. In November 2023, the LockBit ransomware gang posted a sample with proof of the exfiltrated data on its website.

62. LockBit threatened to sell or leak 50 gigabytes of data exfiltrated during the Data Breach unless a $500,000 ransom was paid, stating "McCamish offered 50k USD … If we receive good enough price from anyone we will sell the ~50GB data to you privately with starting bid of 500k… ALL AVAILABLE DATA WILL BE PUBLISHED."

63. IMS began notifying affected individuals with regard to some IMS Clients in February 2024.

64. However, IMS waited to send some personally addressed Notice Letters, months later in June 2024.[11]

---

[8] *See id.*
[9] *See* https://www.cpomagazine.com/cyber-security/infosys-mccamish-systems-lockbit-ransomware-data-breach-impacted-6-million-people-leaked-extensive-pii/.
[10] *Id.*
[11] *See* Notice Letter.

65. In its Notice Letter, Defendant apprised affected individuals "that data was subject to unauthorized access and acquisition," and that the "unauthorized activity occurred between October 29, 2023, and November 2, 2023."[12]

66. The Notice Letter reads:

> Infosys McCamish Systems, LLC ("IMS") writes to inform you of an incident that involved some of your personal information. While we are unaware of any instances since the incident occurred in which the personal information involved has been fraudulently used, we are providing you with information about the incident and steps you can take to protect your personal information, should you feel it necessary to do so.
>
> WHAT HAPPENED? On November 2, 2023, IMS became aware that certain IMS systems were encrypted by ransomware (the "Incident"). That same day, we began an investigation with the assistance of third-party cybersecurity experts, retained through outside counsel, to determine the nature and scope of the activity, assist with containment, and ensure no ongoing unauthorized activity. IMS also promptly notified law enforcement. Please note that the Incident has since been contained and remediated.
>
> The in-depth cyber forensic investigation determined that unauthorized activity occurred between October 29, 2023, and November 2, 2023. Through the investigation, it was also determined that data was subject to unauthorized access and acquisition. With the assistance of third-party eDiscovery experts, retained through outside counsel, IMS proceeded to conduct a thorough and time-intensive review of the data at issue to identify the personal information subject to unauthorized access and acquisition and determine to whom the personal information relates. On May 28, 2024, after a comprehensive review, it was determined that some of your personal information was subject to unauthorized access/ acquisition.[13]

[12] *Id.*

[13] *See* Notice Letter.

67. Defendant did not inform affected individuals of the root cause of the Data Breach beyond reference to the fact that "IMS systems were encrypted by ransomware."[14]

68. Defendant did not disclose that LockBit had threatened to sell or leak 50 gigabytes of data exfiltrated during the Data Breach unless a $500,000 ransom was paid.

69. The notice letter that Bank of America sent to Plaintiff Collins and others stated that IMS told Bank of America that data "may have been compromised," notwithstanding that Lockbit had posted a sample of the exfiltrated data on its website and threatened to publish 50 gigabytes of data exfiltrated during the Data Breach unless a $500,000 ransom was paid.

70. Defendant's Notice Letter stated that it identified individuals whose data was exposed to unauthorized third parties on June 27, 2024.

71. Defendant did not state why more than six months elapsed between discovery of the Data Breach and identification of affected individuals.

72. Defendant did not state why it waited months to inform individuals that their PII was compromised after their identification.

73. Defendant failed to prevent the data breach because it did not adhere to

[14] *Id.*

commonly accepted security standards and failed to detect that its databases were subject to a security breach.

74. Defendant knew and understood that the PII of Plaintiffs and Class Members was provided to it under the condition that it maintain its confidentiality and that it was obliged to implement reasonable data security safeguards.

75. IMS's Privacy Statement represents that, "Infosys adopts reasonable and appropriate security controls, practices and procedures including administrative, physical security, and technical controls in order to safeguard your Personal Information."[15]

76. The Privacy Statement further states that it applies to "Personal Information that we collect and process about you through various sources" and "our adherence to the below mentioned principles remain across the organization towards personal data processing."

77. Accordingly, it is clear that Defendant understood that it was responsible for ensuring that the PII that they collected was reasonably protected with adequate safeguards.

78. Had Defendant implemented basic and industry standard data protection measures, this Data Breach could have been prevented or mitigated.

[15] https://web.archive.org/web/20230801213902/https://www.infosys.com/privacy-statement.html, IMS privacy policy as of August 1, 2023.

79. IMS could and should have encrypted or redacted PII stored on internet accessible network environments, monitored its systems to detect intrusions and prevent continued access, limited remote access to PII to only necessary employees, implemented protocols to contain intrusions, trained employees to detect phishing attacks or other attempts to gain access to security credentials, required multi-factor authentication, and deleted information that it was no longer required to maintain.

80. Defendant's failure to implement these reasonable and expected measures was the direct and proximate cause of their injuries.

B. PLAINTIFFS' INDIVIDUAL EXPERIENCES

Plaintiff John McNally

81. Plaintiff John McNally is, and at all relevant times has been, a resident and citizen of Georgia.

82. Plaintiff McNally was a customer of IMS Client Bank of America.

83. Plaintiff McNally received a Notice Letter from IMS dated February 6, 2024 informing him that his PII was involved in the Data Breach.

84. The Notice Letter Plaintiff McNally received explains: "We are writing to you about a security incident at Infosys McCamish Systems LLC ("IMS"). IMS provides services for deferred compensation plans, including plans serviced by Bank of America that you were eligible to participate in. Out of an abundance of caution, we are notifying you about this incident and providing tools to help you protect

against possible identity theft or fraud."

85. Since the Data Breach, Plaintiff McNally has noticed an increase in spam calls and texts. Moreover, following the Data Breach, Plaintiff experienced fraudulent charges and purchases on his Bank of America Visa card, which had to be replaced due to the incidents.

86. In addition, Plaintiff McNally has been experiencing anxiety, fear and stress as a result of the Data Breach and his PII being disclosed and is fearful of further identity theft and fraud, and of the consequences of such identity theft and fraud resulting from the Data Breach, including of the risk of ruining his credit.

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

88. As a direct and proximate result of the Data Breach, Plaintiff McNally has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect. This is time he would otherwise have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

89. As a result of the Data Breach, Plaintiff McNally anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach. He has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

90. Plaintiff McNally has a continuing interest in ensuring that his PII, which upon information and belief remains backed up in Defendant's possession, is protected and safeguarded from future data breaches.

Plaintiff Patricia Ann Kennemur

91. Plaintiff Patricia Ann Kennemur is, and at all relevant times has been, a resident and citizen of Texas.

92. Plaintiff Kennemur is a customer of IMS Client New York Life Group Benefits Solutions Insurance she receives through her work.

93. Plaintiff Kennemur received two Notice Letters from IMS dated June 27, 2024, and September 5, 2024, informing her that her PII was involved in the Data Breach.

94. The Notice Letter Plaintiff Kennemur received explains: IMS provides a producer compensation and management solution that is used by insurance carriers, including New York Life Group Benefits Solutions.

95. The Notice Letter informed Plaintiff Kennemur that her name, employee ID, personal address, Social Security number, financial account number, and date of birth were compromised in the Data Breach.

96. Since the Data Breach, Plaintiff Kennemur has received alerts from USAA's Fraud Division regarding fraudulent charges placed on her USAA card. Plaintiff Kennemur has experienced fraudulent charges on her USAA card, requiring her to close her account and obtain a new card, four times.

97. In addition, Plaintiff Kennemur has been experiencing anxiety and stress as a result of the Data Breach and her PII being disclosed, and is fearful of further identity theft and fraud, and of the consequences of such identity theft and fraud resulting from the Data Breach, including of the risk of his credit.

98. Plaintiff Kennemur is very careful about sharing sensitive PII. Plaintiff stores any documents containing PII in a safe and secure location and has never knowingly transmitted unencrypted sensitive PII over the Internet or any other unsecured source. Plaintiff would not have entrusted her PII to Defendant had Plaintiff known of Defendant's lax data security policies.

99. As a direct and proximate result of the Data Breach, Plaintiff Kennemur has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. This is time she would otherwise

have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

100. As a result of the Data Breach, Plaintiff Kennemur anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach. She has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

101. Plaintiff Kennemur has a continuing interest in ensuring that her PII, which upon information and belief remains backed up in Defendant's possession, is protected and safeguarded from future data breaches.

Plaintiff Kelly Collins

102. Plaintiff Kelly Collins is, and at all relevant times has been, a resident and citizen of Arkansas.

103. Plaintiff Collins was a customer of IMS Client Bank of America.

104. Plaintiff Collins received a Notice Letter in March 2024 from IMS informing her that her PII was involved in the Data Breach.

105. The Notice Letter Plaintiff Collins received explains: IMS provides a producer compensation and management solution that is used by insurance carriers, including Bank of America.

106. Since the Data Breach, Plaintiff Collins has experienced fraudulent charges on her Bank of America Account, someone taking out a car loan in her name,

having someone claim her grandson on their taxes despite her being his legal guardian, and someone has tried to claim Social Security Benefits in her name.

107. In addition, Plaintiff Collins has been experiencing anxiety and stress as a result of the Data Breach and her PII being disclosed, and is fearful of further identity theft and fraud, and of the consequences of such identity theft and fraud resulting from the Data Breach, including of the risk and actual harm to her credit.

108. Plaintiff Collins is very careful about sharing sensitive PII. Plaintiff stores any documents containing PII in a safe and secure location and has never knowingly transmitted unencrypted sensitive PII over the Internet or any other unsecured source. Plaintiff would not have entrusted her PII to Defendant had Plaintiff known of Defendant's lax data security policies.

109. As a direct and proximate result of the Data Breach, Plaintiff Collins has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring her financial accounts for any indication of fraudulent activity, and changing her financial accounts and cards. This is time she would otherwise have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

110. As a result of the Data Breach, Plaintiff Collins anticipates spending considerably more time and money on an ongoing basis to try to mitigate and address

the harm caused by the Data Breach. She has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

111. Plaintiff Collins has a continuing interest in ensuring that her PII, which upon information and belief remains backed up in Defendant's possession, is protected a safeguarded from future data breaches.

Plaintiff Deana Lindley

112. Plaintiff Deana Lindley is, and at all relevant times has been, a resident and citizen of North Carolina.

113. Plaintiff Lindley was a customer of Continental Casualty Company, her long-term care insurance for the last ten years.

114. Plaintiff Lindley received a Notice Letter from IMS dated June 27, 2024, informing her that her PII was involved in the Data Breach.

115. The Notice Letter Plaintiff Lindley received explains: "IMS provides a producer compensation and management solution that is used by insurance carriers, including Continental Casualty Company."

116. Since the Data Breach, Plaintiff McNally has noticed an increase in spam communications.

117. In addition, Plaintiff Lindley has been experiencing anxiety and stress as a result of the Data Breach and her PII being disclosed, and is fearful of further

identity theft and fraud, and of the consequences of such identity theft and fraud resulting from the Data Breach, including of the risk of her credit.

118. Plaintiff Lindley is very careful about sharing sensitive PII. Plaintiff stores any documents containing PII in a safe and secure location and has never knowingly transmitted unencrypted sensitive PII over the Internet or any other unsecured source. Plaintiff would not have entrusted her PII to Defendant had Plaintiff known of Defendant's lax data security policies.

119. As a direct and proximate result of the Data Breach, Plaintiff Lindley has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring her financial accounts for any indication of fraudulent activity, which may take years to detect. This is time she would otherwise have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

120. As a result of the Data Breach, Plaintiff Lindley anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach. She has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

121. Plaintiff Lindley has a continuing interest in ensuring that her PII, which upon information and belief remains backed up in Defendant's possession, is protected a safeguarded from future data breaches.

Plaintiff Josh Strock

122. Plaintiff Joshua L. Strock is, and at all relevant times has been, a resident and citizen of Georgia

123. Through his employment, Plaintiff Joshua L. Strock received life insurance benefits provided by New York Benefit Life Solutions, from about August 2021 through 2023.

124. Plaintiff Joshua L. Strock received two Notice Letters from IMS dated September 5, 2024, informing him that his PII was involved in the Data Breach. The Notice Letter stated that "[t]he investigation determined that the following types of your personal information were involved: your name, date of birth, employee ID, financial account number, personal address, Social Security number, and client or customer account number / policy number."

125. The Notice Letters Plaintiff Strock received explains: "IMS supports New York Life Group Benefit Solutions' corporate and business market operations, such as administering group benefits and/or sending benefit continuation letters."

126. Since the Data Breach, Plaintiff Strock has noticed an increase in spam communications.

127. In addition, Plaintiff Strock has been experiencing anxiety and stress as a result of the Data Breach and his PII being disclosed, and he is concerned about

identity theft and fraud, and of the consequences of such identity theft and fraud resulting from the Data Breach, including of the risk of ruining his credit.

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

129. As a direct and proximate result of the Data Breach, Plaintiff Strock has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring his financial accounts for any indication of fraudulent activity; by regularly reviewing credit reports; freezing credit with all credit bureaus; routinely changing passwords; running ransomware checks; and by monitoring the dark web. However, the impact may take years to detect. This is time he would otherwise have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

130. As a result of the Data Breach, Plaintiff Strock anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. He has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

131. Plaintiff Strock has a continuing interest in ensuring that his PII, which upon information and belief remains backed up in Defendant's possession, is protected and safeguarded from future data breaches.

Plaintiff Mohamad Raychouni

132. Plaintiff Mohamad Raychouni is, and at all relevant times has been, a resident and citizen of Michigan.

133. Plaintiff Raychouni is unaware how IMS received his PII, however, the Notice Letter he received from IMS states his PII was procured through IMS's relationship with Foresters Financial. Plaintiff Raychouni has never been employed by IMS.

134. Plaintiff Raychouni received a Notice Letter from IMS dated September 26, 2024, informing him that his PII was involved in the Data Breach, specifically his name, financial account number, and Social Security number.

135. The Notice Letter Plaintiff Raychouni received explains: "IMS provides a producer compensation and management solution that is used by insurance carriers, including The Independent Order of Foresters (Foresters Financial)."

136. Since the Data Breach, Plaintiff Raychouni has noticed a significant increase in spam communications, so much so that Plaintiff Raychouni purchased "TrapCall," a spam call blocking service, for $15.00 per month. Plaintiff Raychouni

estimates he receives between 5–20 spam calls per day. Moreover, following the Data Breach Plaintiff Raychouni discovered: (i) multiple fraudulent inquiries on his credit report, which he disputed with Experian; (ii) multiple fraudulent addresses listed on his credit report that he has never been associated with; and (iii) multiple unauthorized charges on three (3) different credit cards, resulting in the credit cards having to be replaced. This is not a coincidence. The acts of fraud and identity theft Plaintiff Raychouni suffered can be perpetrated using the exact information IMS exposed in the Data Breach.

137. In addition, Plaintiff Raychouni is experiencing anxiety, fear, and stress as a result of the Data Breach and his PII being disclosed. Plaintiff Raychouni is fearful of further identity theft and fraud, particularly of the consequences any future identity theft and fraud could have on his credit.

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

139. As a direct and proximate result of the Data Breach, Plaintiff Raychouni has made reasonable efforts to mitigate the impact of the Data Breach, including regularly and closely monitoring his financial accounts and credit reports for

fraudulent activity. Plaintiff Raychouni estimates he has spent between 200–300 hours responding to the ramifications of the Data Breach thus far. This is time he would otherwise have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

140. As a result of the Data Breach, Plaintiff Raychouni anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach. In response to the Data Breach (and the fraud and identity theft he has already experienced), Plaintiff Raychouni purchased three (3) different credit monitoring services, including: (i) Experian Credit Monitoring for $30.00 per month; (ii) Identity IQ for $30.00 per month; and (iii) SmartCredit for $20.00 per month. These are ongoing expenses Plaintiff Raychouni must pay for the rest of his life to protect himself from the fallout of the Data Breach. Plaintiff Raychouni faces a present and continuing risk of fraud and identity theft for his lifetime.

141. Plaintiff Raychouni has a continuing interest in ensuring that his PII, which upon information and belief remains backed up in Defendant's possession, is protected and safeguarded from future data breaches.

Plaintiff Nathaniel Seibert

142. Plaintiff Nathaniel Seibert is, and at all relevant times has been, a resident and citizen of Florida.

143. Plaintiff Seibert is unaware how IMS obtained his PII, but the Notice Letters he received from IMS state he was implicated in the Data Breach through New York Life Group Benefit Solutions. Plaintiff Seibert has never been employed at IMS.

144. Plaintiff Seibert received four Notice Letters from IMS dated September 5, 2024, on behalf of New York Life Group Benefit Solutions informing him that his name, Social Security number, date of birth, employee ID, financial account number, and/or personal address were involved in the Data Breach, and one Notice Letter from IMS (which listed no other entity) dated June 27, 2024, informing him that his name, Social Security number, and financial account number were involved in the Data Breach.

145. Four of the Notice Letters Plaintiff Seibert received explain: "IMS supports New York Life Group Benefits Solutions' corporate and business market operations, such as administering group benefits and/or sending benefit continuation letters."

146. Since the Data Breach, Plaintiff Seibert has noticed an increase in spam communications.

147. In addition, Plaintiff Seibert has been experiencing anxiety, fear, and/or stress as a result of the Data Breach and his PII being disclosed, and is concerned

about future identity theft and fraud, and of the consequences of such identity theft and fraud resulting from the Data Breach, including of the risk of ruining his credit.

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

149. As a direct and proximate result of the Data Breach, Plaintiff Seibert has made reasonable efforts to mitigate the impact of the Data Breach, including: (i) regularly and closely monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect; (ii) researching the facts, background, and legitimacy of the Data Breach; (iii) researching credit monitoring services; and (iv) reviewing his credit reports. This is time he would otherwise have spent on other activities, including but not limited to work and/or recreation. In total, Plaintiff Seibert estimates he has spent approximately 50 hours to date responding to the ramifications of the Data Breach. This time has been lost forever and cannot be recaptured.

150. As a result of the Data Breach, Plaintiff Seibert anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the

harms caused by the Data Breach. He has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

151. Plaintiff Seibert has a continuing interest in ensuring that his PII, which upon information and belief remains backed up in Defendant's possession, is protected and safeguarded from future data breaches.

Plaintiff Joyce Newman

152. Plaintiff Joyce Newman is, and at all relevant times has been, a resident and citizen of New York.

153. Plaintiff Newman was a customer of TIAA and TIAA Life.

154. Plaintiff Newman received a Notice Letter from IMS dated March 7, 2024 informing her that her PII was involved in the Data Breach.

155. The Notice Letter Plaintiff Newman received explains: "We are writing to inform you of a cybersecurity incident that occurred at Infosys McCamish Systems, LLC ("IMS"), one of TIAA and TIAA Life's administrative support services providers, as it relates to your personal information. IMS has informed us that some of your personal information was involved in this incident".

156. Since the Data Breach, Plaintiff Newman has experienced an increase in spam texts, emails and calls. Furthermore, after the data breach, the plaintiff experienced a fraudulent charge on a visa card, which was subsequently replaced.

157. In addition, Plaintiff Newman has been experiencing anxiety, fear and

stress as a result of the Data Breach and his PII being disclosed and is fearful and concerned about further identity theft and fraud, and of the consequences of such identity theft and fraud resulting from the Data Breach, including of the risk of ruining her credit.

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

159. As a direct and proximate result of the Data Breach, Plaintiff Newman has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect, and she has spent approximately 20 hours monitoring her accounts. This is time she would otherwise have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

160. As a result of the Data Breach, Plaintiff Newman anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. She has faced and faces a present and continuing risk of fraud and identity theft for her lifetime.

161. Plaintiff Newman has a continuing interest in ensuring that her PII, which upon information and belief remains backed up in Defendant's possession, is protected and safeguarded from future data breaches.

Plaintiff Andrew Snaith

162. Plaintiff Andrew Snaith is, and at all relevant times has been, a resident and citizen of Pennsylvania.

163. Plaintiff Snaith was a customer of New York Life Group Benefits Solutions.

164. Plaintiff Snaith received a Notice Letter from IMS dated September 5, 2024, informing him that his PII was involved in the Data Breach.

165. The Notice Letter Plaintiff Snaith received explains: "Infosys McCamish Systems, LLC ("IMS") writes to inform you of an incident that involved some of your personal information. IMS supports New York Life Group Benefit Solutions' corporate and business market operations, such as administering group benefits and/or sending benefit continuation letters. While we are unaware of any instances since the incident occurred in which the personal information involved has been fraudulently used, we are providing you with information about the incident and steps you can take to help protect your personal information, should you feel it necessary to do so".

166. Since the Data Breach, Plaintiff Snaith has noticed increase in spam

texts. Moreover, following the Data Breach, Plaintiff experienced fraudulent charges of hundreds worth of items on his debit cards.

167. In addition, Plaintiff Snaith has been experiencing anxiety and fear as a result of the Data Breach and his PII being disclosed and is fearful of further identity theft and fraud and of the consequences of such identity theft and fraud resulting from the Data Breach, including of the risk of ruining his credit.

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

169. As a direct and proximate result of the Data Breach, Plaintiff Snaith has made reasonable efforts to mitigate the impact of the Data Breach, including by regularly and closely monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect, and had to cancel three debits' cards due fraudulent charges and unauthorized activity on debit/credit cards and bank accounts. Plaintiff Snaith has spent hours monitoring his accounts due to suspicious activity. This is time he would otherwise have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

170. As a result of the Data Breach, Plaintiff Snaith anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harm caused by the Data Breach. He has faced and faces a present and continuing risk of fraud and identity theft for his lifetime.

171. Plaintiff Snaith has a continuing interest in ensuring that his PII, which upon information and belief remains backed up in Defendant's possession, is protected and safeguarded from future data breaches.

C. Defendant Was on Notice of Data Threats in the Industry and of the Inadequacy of Its Data Security Systems

172. Defendant was on notice that companies that maintain large amounts of PII are prime targets for criminals looking to gain unauthorized access to sensitive and valuable information.

173. At all relevant times, Defendant knew, or should have known, that the PII that it collected was a target for malicious actors. Despite such knowledge, IMS failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class Members' PII from cyber-attacks that IMS should have anticipated and guarded against.

174. It is well known among companies that store sensitive personally identifying information that sensitive information—such as the Social Security numbers stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all

kinds of businesses, including retailers . . . Many of them were caused by flaws in . . . systems either online or in stores."[16]

175. Additionally, in the third quarter of the 2023 fiscal year alone, 7333 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information being compromised.[17]

176. In light of recent high profile data breaches, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), Advanced Info Service (8.3 billion records, May 2020), and Morgan Stanley Smith Barney LLC (15 million customers), IMS knew or should have known that its electronic records would be targeted by cybercriminals.

177. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, take appropriate measures to prepare for, and are able to thwart such an attack.

---

[16] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

[17] *See* https://www.idtheftcenter.org/publication/q3-data-breach-2023-analysis/ (last accessed Oct. 11, 2023).

178. Additionally, as companies became more dependent on computer systems to run their business,[18] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[19]

179. Defendant knew and understood unprotected or exposed PII in its custody is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

180. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members and of the foreseeable consequences that would occur if its 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.

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

---

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

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

182. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant' failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

183. Moreover, PII is a valuable property right.[20] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[21] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[22] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

184. As a result of their real and significant value, identity thieves and other cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites making the

[20] *See* Marc van Lieshout, *The Value of Personal Data*, 457 International Federation for Information Processing 26 (May 2015) ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible…"), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data

[21] OECD, *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD LIBRARY (April 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[22] IAB Data Center of Excellence, *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, IAB.COM (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be readily aggregated and become more valuable to thieves and more damaging to victims.

185. Consumers place a high value on the privacy of that data, as they should. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[23]

186. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

D. Cyber Criminals Will Use Plaintiffs' and Class Members' PII to Defraud Them

187. Plaintiffs' and Class Members' PII is of great value to cyber criminals, and the data stolen in the Data Breach has already been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and the Class Members and to profit off their misfortune.

[23] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011) https://www.jstor.org/stable/23015560?seq=1.

188. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[24]

189. For example, with the PII stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[25]

190. These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class Members.

191. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[26]

---

[24] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[25] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/

[26] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/products/gao-07-737

192. For example, it is believed that certain highly sensitive personal information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related unemployment benefits.[27]

193. The PII exposed in this Data Breach is valuable to identify thieves for use in the kinds of criminal activity described herein. These risks are both certainly impending and substantial. As the FTC has reported, if cyber thieves get access to a person's highly sensitive information, they will use it.[28]

194. Cyber criminals may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

195. [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[29]

---

[27] *See* https://www.engadget.com/stolen-data-used-for-unemployment-fraud-ring-174618050.html; *see also* *https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/*.

[28] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[29] *Data Breaches Are Frequent*, *supra* note 14.

196. For instance, with a stolen Social Security number, which is only one category of the PII compromised in the Data Breach, someone can open financial accounts, file fraudulent tax returns, commit crimes, and steal benefits.[30]

197. Victims of the Data Breach, like Plaintiffs and other Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[31]

198. In fact, as a direct and proximate result of the Data Breach, Plaintiffs and the Class have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs and the Class must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank

[30] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/

[31] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf

accounts, credit reports, and other information for unauthorized activity for years to come.

199. Plaintiffs and the Class have suffered or will suffer actual harms for which they are entitled to compensation, including but not limited to the following:

a. Trespass, damage to, and theft of their personal property, including PII;
b. Improper disclosure of their PII;
c. The imminent and certainly impending injury flowing from actual and potential future fraud and identity theft posed by their PII being in the hands of criminals and having already been misused;
d. The imminent and certainly impending risk of having their confidential information used against them by spam callers to defraud them;
e. Damages flowing from IMS's untimely and inadequate notification of the Data Breach;
f. Loss of privacy suffered as a result of the Data Breach;
g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;
h. Ascertainable losses in the form of deprivation of the value of individuals' personal information for which there is a well-established and quantifiable national and international market;
i. The loss of use of and access to their credit, accounts, and/or funds;
j. Damage to their credit due to fraudulent use of their PII; and
k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

200. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII, which remains in the possession of Defendant, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendant have shown itself to be wholly incapable of protecting Plaintiffs' and Class Members' PII.

201. Plaintiffs and Class Members are trying to mitigate the damage that Defendant has caused them but, given the kind of PII Defendant made so easily accessible to cyber criminals, they are certain to incur additional damages. Because identity thieves already have their PII, Plaintiffs and Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with this change.[32]

E. Defendant Could Have Prevented the Data Breach but Failed to Adequately Protect Plaintiffs' and Class Members' PII

202. Data disclosures and data breaches are preventable.[33] As Lucy

[32] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html

[33] 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, "In 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."[34] 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 . . . ."[35]

203. "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*."[36]

204. Defendant obtained and stored Plaintiffs' and Class Members' PII—including their Social Security numbers—and was entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of such PII.

205. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting its equipment and computer files containing PII.

[34] *Id.* at 17.
[35] *Id.* at 28.
[36] *Id.*

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

207. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[37]

208. To prevent and detect cyber-attacks and/or ransomware attacks IMS 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, customers 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.

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

- 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.[38]

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

Secure internet-facing assets

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

- 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].[39]

210. Given that Defendant collected and stored the PII of Plaintiffs and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

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

F. Value of Personally Identifiable Information

211. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[40] 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."[41]

212. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[42] For example, PII can be sold at a price ranging from $40 to $200.[43] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[44]

---

[40] 17 C.F.R. § 248.201 (2013).
[41] *Id.*
[42] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.
[43] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Oct. 17, 2022).
[44] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/

213. PII can sell for as much as $363 per record according to the Infosec Institute.[45] PII is particularly valuable because criminals can use it to target victims with frauds and scams.

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

215. 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 being issued in the victim's name.

216. 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.

[45] *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/

217. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when 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 have 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.[46]

218. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[47] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[48]

219. Each of these fraudulent activities is difficult to detect. An individual may not know that her or her Social Security Number was used to file for

---

[46] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* https://www.gao.gov/assets/gao-07-737.pdf.
[47] *Identity Theft and Your Social Security Number*, Social Security Administration (2018). Available at https://www.ssa.gov/pubs/EN-05-10064.pdf.
[48] *Id*.

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.

220. Moreover, it is not an easy task to change or cancel a stolen Social Security number:

> An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[49]

221. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[50]

222. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card

[49] 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.

[50] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

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—Social Security numbers.

G. Defendant Failed to Comply with FTC Guidelines

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

224. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[51]

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

225. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[52]

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

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

228. These FTC enforcement actions include actions against lending companies, like IMS.

[52] *Id.*

229. Defendant failed to properly implement basic data security practices.

230. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

231. Upon information and belief, Defendant was at all times fully aware of its obligation to protect PII. Defendant was also aware of the significant repercussions that would result from its failure to do so.

H. IMS Fails To Comply With Industry Standards

232. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

233. Several best practices have been identified that, at a minimum, should be implemented by lending companies in possession of PII, like IMS, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. IMS failed to follow these industry best practices, including a failure to implement multi-factor authentication.

234. Other best cybersecurity practices that are standard in the lending 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; training staff regarding critical points. IMS failed to follow these cybersecurity best practices, including failure to train staff.

235. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

236. These foregoing frameworks are existing and applicable industry standards in the lending industry, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

I. Common Injuries & Damages

237. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members

has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their PII; (e) invasion of privacy; and (f) the continued risk to their PII, which remains in the possession of IMS, and which is subject to further breaches, so long as IMS fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' PII.

The Data Breach Increases Victims' Risk Of Identity Theft

238. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come.

239. As multiple Plaintiffs have already experienced, the unencrypted PII of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted PII may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

240. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal PII to monetize the information. Criminals monetize the data by selling the stolen information on the black market to

other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

241. 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.

242. 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 can be the starting point for these additional targeted attacks on the victim.

243. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[53]

[53] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions

244. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

245. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

---

over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on May 26, 2023).

246. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

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

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

Loss Of Time To Mitigate Risk Of Identity Theft And Fraud

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

250. Thus, due to the actual and imminent risk of identity theft, IMS encourages Plaintiffs and Class Members to do the following:

> We encourage you to remain vigilant against identity theft and fraud by reviewing your financial account statements and credit reports for any

> anomalies and encourage you to notify your financial institution of any unauthorized transactions or suspected identity theft. We also encourage you to review the enclosed Additional Steps to Protect Your Personal Information and State Law Information for additional guidance. You should be on guard for schemes where malicious actors may pretend to represent IMS or reference this Incident.[54]

251. 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/or otherwise securing their financial accounts; contacting banks to sort out fraudulent activity; signing up for credit monitoring and identity theft insurance; checking if their information was exposed on the dark web; and monitoring their financial accounts for any indication of fraud, which may take years to detect.

252. 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]

253. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit

[54] Notice Letter.

[55] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[56]

254. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[57]

Diminution Value Of PII

255. PII is a valuable property right.[58] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

---

[56] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited July 7, 2022).

[57] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Sep. 13, 2022) ("GAO Report").

[58] *See, e.g.,* Randall 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).

256. An active and robust legitimate marketplace for PII exists. In 2019, the data brokering industry was worth roughly $200 billion.[59]

257. 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.[60,61]

258. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[62]

259. Conversely, sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[63]

260. As a result of the Data Breach, Plaintiffs' and Class Members' PII, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the PII is now

[59] https://www.latimes.com/business/story/2019-11-05/column-data-brokers
[60] https://datacoup.com/
[61] https://digi.me/what-is-digime/
[62] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html
[63] *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 Sep. 13, 2022).

readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

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

262. 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.

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

264. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if IMS'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.

265. The injuries to Plaintiffs and Class Members were directly and

proximately caused by IMS's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

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

266. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PII involved, the volume of data obtained in the Data Breach, and multiple Plaintiffs' PII already being disseminated on the dark web (as discussed above), there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes –*e.g.,* opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

267. 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.

268. 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.[64] The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

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

270. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from IMS's Data Breach.

Loss Of The Benefit Of The Bargain

271. Furthermore, Defendant's poor data security practices deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay IMS' Clients for services, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying for the service and necessary data security to protect the PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser

[64] *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.

value than what they reasonably expected to receive under the bargains they struck with Defendant.

CLASS ALLEGATIONS

272. Plaintiffs bring this class action individually on behalf of themselves and on behalf of all members of the following Class of similarly situated persons pursuant to Federal Rule of Civil Procedure 23. Plaintiffs seek certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3) of the following Class:

Nationwide Class

All persons residing in the United States whose PII was compromised in the Data Breach, including all who were sent a notice of the Data Breach.

(hereafter, the "Nationwide Class" or the "Class").

273. Excluded from the Class are Defendant and its affiliates, parents, subsidiaries, officers, agents, and directors, any entities in which Defendant has a controlling interest, as well as the judge(s) presiding over this matter and the clerks, judicial staff, and immediate family members of said judge(s).

274. Plaintiffs reserve the right to modify or amend the foregoing class definitions before the Court determines whether certification is appropriate.

275. **Numerosity:** The members in the Class are so numerous that joinder of all Class Members in a single proceeding would be impracticable. As noted above, it has been reported that approximately 6,078,263 individuals' information was compromised and exposed in the Data Breach.

276. **Commonality and Predominance:** Common questions of law and fact exist as to all Class Members and predominate over any potential questions affecting only individual Class Members. These common questions of law or fact include, *inter alia*:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiffs' and Class Members' PII from unauthorized access and disclosure;

c. Whether Defendant's computer systems and data security practices used to protect Plaintiffs' and Class Members' PII violated the FTC Act and/or state laws, and/or Defendant's other duties discussed herein;

d. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiffs and Class Members;

e. Whether Defendant unlawfully shared, lost, or disclosed Plaintiffs' and Class Members' PII;

f. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether Plaintiffs and Class Members suffered injury as a proximate result of Defendant's negligent actions or failures to act;

i. Whether Defendant failed to exercise reasonable care to secure and safeguard Plaintiffs' and Class Members' PII;

j. Whether Defendant breached duties to protect Plaintiffs' and Class Members' PII;

k. Whether Defendant's actions and inactions alleged herein were negligent;

l. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages or other relief, and the measure of such damages and relief;

m. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

n. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief.

277. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs on behalf of themselves and all other Class Members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

278. **Typicality:** Plaintiffs' claims are typical of the claims of the Class. Plaintiffs, like all proposed members of the Class, had their PII compromised in the Data Breach. Plaintiffs and Class Members were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiffs' claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class Members.

279. **Adequacy:** Plaintiffs will fairly and adequately protect the interests of the Class. Plaintiffs are adequate representatives of the Class and have no interests adverse to, or in conflict with, the Class they seek to represent. Plaintiffs have retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

280. **Superiority:** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiffs and all other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for Class Members to individually seek redress from Defendant's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

281. **Injunctive and Declaratory Relief:** Defendant has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive

relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

282. All members of the proposed Class are readily ascertainable. Defendant has access to the names in combination with addresses and/or e-mail addresses of Class Members affected by the Data Breach. Indeed, impacted Class Members already have been preliminarily identified and sent a breach Notice Letter.

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

283. Plaintiffs restate and reallege paragraphs 1 through 282 above as if fully set forth herein.

284. All Plaintiffs bring this Count on their own behalf and on behalf of the Nationwide Class against Defendant IMS.

285. Defendant gathered and stored the PII of Plaintiffs and the Class as part of the operation of its business. Defendant utilized a shared network on which the PII of Plaintiffs and Class Members was stored and was subject to common data security policies governing the collection, use, sharing, and retention of Plaintiffs' and Class Members' PII (including, but not limited to InfoSys's Privacy Statement).

286. Upon accepting and storing the PII of Plaintiffs and Class Members, Defendant undertook and owed a duty to Plaintiffs and Class Members to exercise

reasonable care to secure and safeguard that information and to use secure methods and to implement necessary data security protocols and employee training to do so.

287. Defendant had full knowledge of the sensitivity of the PII, the types of harm that Plaintiffs and Class Members could and would suffer if the PII was wrongfully disclosed, and the importance of adequate security.

288. Plaintiffs and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class Members had no ability to protect their PII that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiffs and the Class.

289. Defendant owed Plaintiffs and Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing their PII, including acting reasonably to safeguard such data and providing notification to Plaintiffs and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

290. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous

courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

291. Defendant had duties to protect and safeguard the PII of Plaintiffs and the Class from being vulnerable to compromise by taking common-sense precautions when dealing with sensitive PII. Additional duties that Defendant owed Plaintiffs, and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class Members' PII was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiffs' and Class Members' PII in their possession by using reasonable and adequate security procedures and systems; and

c. To promptly notify Plaintiffs and Class Members of any breach, security incident, unauthorized disclosure, or intrusion that affected or may have affected their PII.

292. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the PII that had been entrusted to it. Plaintiffs relied on Defendant to exercise its judgment with respect to implementing reasonable data security standards and had no way to influence those standards or verify their integrity.

293. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and Class Members' PII. Defendant breached its duties by, among other

things:

a. Failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting the PII in its possession;

b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees and/or clients regarding how to properly and securely transmit and store PII;

d. Failing to adequately train its employees to not store unencrypted PII in their personal files longer than absolutely necessary for the specific purpose that it was sent or received;

e. Failing to consistently enforce security policies aimed at protecting Plaintiffs' and the Class's PII;

f. Failing to mitigate the harm caused to Plaintiffs and the Class Members;

g. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

h. Failing to promptly notify its clients, Plaintiffs, and Class Members of the Data Breach that affected their PII.

294. IMS could and should have encrypted or redacted PII stored on internet accessible network environments, monitored its systems to detect intrusions and prevent continued access, limited remote access to PII to only necessary employees, implemented protocols to contain intrusions, trained employees to detect phishing attacks or other attempts to gain access to security credentials, required multi-factor authentication, and deleted information that it was no longer required to maintain.

295. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

296. As a proximate and foreseeable result of Defendant's negligent conduct, Plaintiffs and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

297. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the PII of Plaintiffs and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiffs and Class Members while it was within Defendant's possession and control.

298. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class Members, Defendant prevented Plaintiffs and Class Members from taking meaningful, proactive steps to secure their PII and mitigate damages.

299. As a result of the Data Breach, Plaintiffs and Class Members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to the fraudulent use of the PII, and closely reviewing and monitoring bank accounts, credit reports, and financial statements.

300. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

301. The damages Plaintiffs and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's negligent conduct.

302. Plaintiffs and the Class have suffered injury and are entitled to actual damages (including general and nominal damages) in amounts to be proven at trial.

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

303. Plaintiffs restate and reallege paragraphs 1 through 282 above as if fully set forth herein.

304. All Plaintiffs bring this Count on their own behalf and on behalf of the Nationwide Class against Defendant IMS.

305. 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 use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

306. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards.

Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach.

307. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

308. Plaintiffs and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect and the harm resulting from the Data Breach is the type of harm the statute was intended to protect against.

309. Defendant's unreasonable data security measures and failure to timely notify Plaintiffs and the Class of the Data Breach violates 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.

310. 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.

311. Defendant's implementation of inadequate data security measures, its failure to resolve vulnerabilities and deficiencies, and its abdication of its responsibility to reasonably protect the PII that the IMS Clients required Plaintiffs and Class Members to provide, and it stored constitutes a violation of the Georgia Constitution and the Restatement of the Law of Torts (Second).

312. Moreover, the harm that has occurred is the type of harm that the FTC Act (and similar state statutes), the Georgia Constitution and the Restatement of the Law of Torts (Second), were intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

313. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have been injured as described herein and throughout this Complaint, and are entitled to damages, including compensatory, punitive, general, and/or nominal damages, in an amount to be proven at trial.

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

314. Plaintiffs restate and re-allege paragraphs 1 through 282 above as if fully set forth herein.

315. All Plaintiffs bring this Count on their own behalf and on behalf of the Nationwide Class against Defendant IMS.

316. 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 grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

317. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and the Class's PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and the Class from further data breaches that compromise their PII. Plaintiffs allege that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Plaintiffs and the Class continue to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future. It is unknown what specific measures and changes Defendant has undertaken in response to the Data Breach.

318. Plaintiffs and the Class have an ongoing, actionable dispute arising out of Defendant's inadequate security measures, including (i) Defendant's failure to encrypt Plaintiffs' and the Class's PII while storing it in an Internet-accessible environment, (ii) Defendant's failure otherwise safeguard and protect the PII, and

(iii) Defendant's failure to delete any PII it no longer had a reasonable need to maintain.

319. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure the PII of Plaintiffs and Class Members.

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure the PII; and

c. Defendant's ongoing breaches of its legal duties continue to cause harm to Plaintiffs and the Class.

320. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendant to: implement reasonable data security safeguards sufficient to protect such PII, to delete any such PII it no longer has a reasonable need to maintain, and implement annual data security audits.

321. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach. The risk of another such breach is real, immediate, and substantial. If another

breach occurs, Plaintiffs and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

322. The hardship to Plaintiffs and the Class if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiffs and the Class will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a legal obligation to employ such measures.

323. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing or mitigating another data breach, thus eliminating or mitigating the additional injuries that would result to Plaintiffs and the Nationwide Class and others whose confidential information would be further compromised.

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

324. Plaintiffs re-allege and incorporate by reference the allegations contained in Paragraphs 1 through 282 above as if fully set forth herein.

325. All Plaintiffs bring this Count on their own behalf and on behalf of the Nationwide Class against Defendant IMS.

326. 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.

327. Section 5 of the FTC Act prohibits "unfair…practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as Defendant for failing to implement and use reasonable measures to protect PII.

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

329. 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.

330. 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.

331. 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).

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

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

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

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

336. 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 V
BREACH OF FIDUCIARY DUTY
(On Behalf of all Plaintiffs and the Nationwide Class)

337. Plaintiffs restate and reallege paragraphs 1 through 282 above as if fully set forth herein.

338. Plaintiffs and Class Members have an interest, both equitable and legal, in the PII about them that was conveyed to, collected by, and maintained by IMS and that was ultimately accessed or compromised in the Data Breach.

339. IMS has a fiduciary relationship with Plaintiffs and Class Members because once it accepted Plaintiffs' and Class Members' PII, it was in the best position to prevent the Data Breach and Plaintiffs and Class Members relied on IMS to exercise its judgment with respect to protecting their PII and preventing unauthorized access.

340. Because of that fiduciary relationship, IMS was provided with and stored valuable PII related to Plaintiffs and Class Members. Plaintiffs and Class

Members expected their information would remain confidential while in Defendant's possession.

341. In light of the special relationship between IMS and Plaintiffs and Class Members, IMS became a fiduciary by undertaking a guardianship of the PII to act primarily for Plaintiffs and Class Members, (a) for the safeguarding of Plaintiffs' and Class Members' PII; (b) to timely notify Plaintiffs and Class Members of a Data Breach and disclosure; and (c) to maintain complete and accurate records of what information (and where) IMS stored that information.

342. IMS had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of its relationship with its clients' customers, in particular, to keep secure their PII as IMS was in an excusive position to implement sufficient data security safeguards and Plaintiffs and Class Members had no way to verify the integrity of IMS's measures and relied on IMS to exercise its judgment with respect to those measures.

343. Plaintiffs and Class Members did not consent to nor authorize IMS to release or disclose their PII to unauthorized third parties.

344. As a direct and proximate result of IMS's breach of its fiduciary duty, Plaintiffs and Class Members are entitled to compensatory, consequential, and general damages suffered as a result of the Data Breach, or in the alternative, nominal damages.

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 against IMS)

345. Plaintiffs restate and reallege paragraphs 1 through 282 above as if fully set forth herein.

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

347. IMS 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.

348. IMS 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' PII, which was a direct and proximate cause of the Data Breach;

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

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

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

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

f. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class

Members' PII, 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' PII; and

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

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

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

351. IMS intended to mislead Plaintiffs and Class Members and induce them to rely on its misrepresentations and omissions.

352. Plaintiffs and Class Members relied on IMS to advise them if its data security and data storage systems were not adequately secure to protect their PII.

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

354. Plaintiffs and Class Members relied to their detriment on IMS's misrepresentations and deceptive omissions regarding its data security practices.

355. Had IMS 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 IMS with their PII.

356. IMS 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 IMS on notice that its security and privacy protections were inadequate.

357. Had IMS disclosed to Plaintiffs and Class Members that its data systems were not secure and, thus, vulnerable to attack, IMS 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, IMS was trusted with sensitive

and valuable PII regarding thousands of persons, including Plaintiffs the Class. IMS 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 IMS held itself out as maintaining a secure platform for PII, Plaintiffs and the Class acted reasonably in relying on IMS's misrepresentations and omissions, the truth of which they could not have discovered.

358. As a direct and proximate result of IMS'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 PII, the imminent and substantially increased risk of fraud and identity theft, and the need to dedicate future expenses and time to protect themselves against further loss.

359. To date, IMS 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' PII from future compromise. As a result, Plaintiff and Class Members remain uninformed and confused as to the adequacy of IMS's data security and IMS's ability to protect the PII entrusted to it. Without adequate improvements,

Plaintiffs' and Class Members' PII remains at an unreasonable risk of future compromise.

360. IMS, 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' PII. Such continued representations and implications, without disclosure of the full scope of the Data Breach or IMS'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 IMS's data security measures have been improved since the Data Breach. By all available measures, IMS's data security practices and systems have not been adequately improved, and Plaintiffs and Class Members remain at an unreasonable risk from future cyberattacks.

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

362. 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). IMS willfully engaged in deceptive trade practices knowing them to be deceptive. IMS knew or should have known that its data security practices were deficient. IMS was aware that entities responsible for collecting and maintaining large amounts of PII, including Social Security numbers, are frequent targets of sophisticated cyberattacks. IMS knew or should have known that its data security practices were insufficient to guard against those attacks.

363. 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.

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

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of all other members of the Class, respectfully request that the Court enter judgment in Plaintiffs' favor and against Defendant as follows:

A. Certifying the Class(es) as requested herein, designating Plaintiffs as Class representatives, and appointing Plaintiffs' counsel as Class Counsel;

B. Awarding Plaintiffs and Class Members appropriate monetary relief, including actual damages, punitive damages, general damages, and nominal damages;

C. Awarding Plaintiffs and Class Members equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiffs, on behalf of themselves and the class, seek appropriate injunctive relief designed to prevent Defendant from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

D. Awarding Plaintiffs and Class Members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiffs and Class Members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiffs and Class Members such other favorable relief as allowable under law.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury of all claims in this Complaint so triable.

[*Signatures to follow on next page*.]

Dated: November 7, 2024.

Respectfully Submitted,

By: *J. Cameron Tribble*
J. Cameron Tribble
Georgia Bar No. 754759
THE BARNES LAW GROUP, LLC
31 Atlanta Street
Marietta, GA 30060
Telephone: (770) 227-6375
Facsimile: (770) 227-6373
Email: ctribble@barneslawgroup.com
Interim Liaison Counsel

Patrick A. Barthle II*
Florida Bar No. 99286
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 229-4023
Facsimile: (813) 222-4708
Email: pbarthle@ForThePeople.com

Gary M. Klinger*
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Telephone: (866) 252-0878
Facsimile: (865) 522-0049
Email: gklinger@milberg.com

Kevin Laukaitis*
LAUKAITIS LAW LLC
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
Telephone: (215) 789-4462
Email: klaukaitis@laukaitislaw.com
Interim Co-Lead Counsel

Ryan D. Maxey*
MAXEY LAW FIRM, P.A.
107 N. 11th St. #402
Tampa, Florida 33602
(813) 448-1125
Email: ryan@maxeyfirm.com

Jeff Ostrow*
KOPELOWITZ OSTROW P.A.
One West Las Olas Boulevard, Suite 500
Fort Lauderdale, FL 33301
Telephone: (954) 525-4100
Email: ostrow@kolawyers.com

Jeffrey Goldenberg*
GOLDENBERG SCHNEIDER, L.P.A.
4445 Lake Forest Drive, Suite 490
Cincinnati, Ohio 45242
Telephone: 513-345-8297
Email: jgoldenberg@gs-legal.com

Charles E. Schaffer*
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Telephone: (215) 592-1500
Facsimile: (215) 592-4663
Email: cschaffer@lfsblaw.com

William B. Federman*
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, Oklahoma 73120
Tel: (405) 235-1560
Fax: (405) 239-2112
wbf@federmanlaw.com
Interim Executive Committee

**Admitted pro hac vice*

CERTIFICATE OF SERVICE AND TYPE SIZE COMPLIANCE

Pursuant to Local Rule 5.1(A), I hereby certify that on this date I electronically filed the foregoing document with the Clerk of Court using the CM/ECF system which will automatically send email notification to all counsel of record. I further certify that the foregoing was prepared compliance with the formatting requirements of Local Rule 5.1, including by the use of Times New Roman (14-point) font.

This 7th day of November, 2024.

Respectfully submitted,

/s/ J. Cameron Tribble
J. Cameron Tribble
Georgia Bar No. 754759

BARNES LAW GROUP, LLC
31 Atlanta Street
Marietta, GA 30060
Telephone: (770-227-6375
Facsimile: (770) 227-6373
E-Mail: ctribble@barneslawgroup.com