Exhibit A

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

PATRICK DUNN, *et al*., individually and on behalf of all others similarly situated, Plaintiffs, v. COMPLETE PAYROLL SOLUTIONS, LLC, Defendant.	**CASE NO. 1:25-cv-30045-LTS** **CONSOLIDATED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Patrick Dunn, Patricia Brown, Eric Marcial, Sokankelly Lim, Patrick Nowak, Carolyn Strycharz, and James Connors ("Plaintiffs") bring this action individually and on behalf of all others similarly situated against Defendant Complete Payroll Solutions, LLC ("CPS" or "Defendant"). Plaintiffs seek to obtain damages, restitution, and injunctive relief for a class of individuals ("Class" or "Class Members") who are similarly situated and have received notices of the Data Breach from CPS. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record.

I. NATURE OF THE ACTION

1. This class action arises out of CPS's failure to properly secure, safeguard, encrypt, and/or timely and adequately destroy Plaintiffs' and Class Members' sensitive personal identifiable information that it had acquired and stored for its business purposes.

2. Defendant's data security failures allowed a targeted cyberattack/ransomware attack between February 21 and March 10, 2024 to compromise Defendant's network (the "Data

Breach" or "Breach") that contained the personally identifiable information ("PII") and protected health information ("PHI") (collectively, "Private Information") of Plaintiffs and other individuals ("the Class").

3. According to Defendant, on or about March 10, 2024, Defendant became aware of suspicious activity on its network and launched an investigation which confirmed that an unauthorized actor accessed its system and may have copied and exfiltrated certain files containing Plaintiffs' and Class Members' Private Information.

4. CPS reported to the Attorney General of Texas's website that the data exfiltrated from its network includes: names, addresses, Social Security numbers, driver's license numbers, financial information (*e.g.*, account number, credit or debit card number), and health insurance information.[1]

5. It was later revealed that the Breach was perpetrated by the Meow group, a well-known ransomware group, that had accessed Defendant's information network and exfiltrated over three GB of data from Defendant's network related to at least 22,000 individuals.[2]

6. Meow later posted the breached data for sale on its leak site.[3] To prove its possession of the breached data, the Meow group also posted sample images of documents stolen from CPS.[4]

---

[1] *Complete Payroll Solutions*, *Data Security Breach Reports*, ATT'Y GEN. OF TEX. (Apr. 29, 2025), https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (last visited July 3, 2023).

[2] *Complete Payroll Solutions*, *Data Breach Notifications*, ME. ATT'Y GEN. (Oct. 23, 2024), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/ece1a563-aa70-4247-b2b7-0fe1370174d5.html (last visited July 3, 2025); Paul Bischoff, *Complete Payroll Solutions notifies 22K+ people of 2024 data breach that leaked SSNs*, COMPARITECH (Apr. 29, 2025), https://www.comparitech.com/news/complete-payroll-solutions-notifies-22k-people-of-2023-data-breach-that-leaked-ssns/ (last visited July 3, 2025).

[3] *Id.*

[4] *Id.*

7. Meow states that the stolen data, which is now for sale, includes employee data, client information, scanned payment documents, personal data (including "dates of birth, social security numbers"), tax documents, payment records, and more.[5]

8. Despite learning of the Data Breach on or about March 10, 2024 and determining that Private Information was compromised, Defendant did not send notices of the Data Breach (the "Notice of Data Breach Letter" or "Notice Letter") to some victims until April 25, 2025.[6]

9. CPS (a third-party human resource, benefits, and payroll administrator) holds and stores certain highly sensitive Private Information of Plaintiffs and putative Class Members, who are individuals enrolled in employment insurance benefits administered by CPS, *i.e.*, individuals who provided their highly sensitive and private information in exchange for employment and/or business services.

10. As a result of the Data Breach, Plaintiffs and thousands of Class Members suffered ascertainable losses in the form of financial losses resulting from identity theft, out-of-pocket expenses, the loss of the benefit of their bargain, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

11. Plaintiffs' and Class Members' highly sensitive personal information—which was entrusted to Defendant—who claims that the "confidentiality, privacy, and security of information in our care is one of our highest priorities"[7]—was compromised and unlawfully accessed and extracted during the Data Breach.

---

[5] *Id.*
[6] *See* Plaintiffs' Notice Letter, Exhibit A. Based on the Notice Letter and State websites, the extent of the Breach was discovered in stages on separate dates and notice of the Breach was given on multiple, separate dates. *See id.* and *Complete Payroll Solutions*, *Data Breach Notifications*, ME. ATT'Y GEN., *supra* note 2.
[7] *Id.*

12. Based upon CPS's Notice Letter, the Private Information compromised in the Data Breach was intentionally accessed and removed, also called exfiltrated, by the cybercriminals who perpetrated this attack and remains in the hands of those cybercriminals.

13. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiffs' and Class Members' Private Information.

14. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. The mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant. Thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

15. Defendant disregarded the privacy and property 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' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members prompt and accurate and complete notice of the Data Breach.

16. Had Defendant properly secured its network, Defendant could have prevented or discovered the intrusion sooner and avoided or mitigated the injuries to Plaintiffs and the Class.

17. Plaintiffs' and Class Members' identities are now at substantial and imminent risk of fraud and identity theft due to Defendant's negligent conduct since the Private Information that

Defendant collected and maintained (including Social Security numbers) is now in the hands of data thieves.

18. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, filing false medical claims 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.

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

20. Upon information and belief, Plaintiffs' and Class Members' Private information is now for sale on the dark web as a result of the Data Breach.[8]

21. As a result of the Data Breach, Plaintiffs and Class Members suffered concrete injuries including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of their Private Information; (iv) lost time (which could have been dedicated to work and recreation) and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) actual misuse of the compromised data, including

[8] In addition to the fact that Meow has posted the breached data for sale on its leak site, typically, in a ransomware attack, the criminal actor will not only encrypt the victim's system and block access until a ransom is paid but also exfiltrate data and threaten to release it to the dark web in what is known as a double-extortion attack. This is because many "organizations overcome the threat of file encryption with a simple up-to-date backup system." *What is Multi-Extortion Ransomware?*, PALO ALTO NETWORKS, https://www.paloaltonetworks.com/cyberpedia/what-is-multi-extortion-ransomware (last visited July 3, 2025).

actual and attempted fraud and identity theft and an increase in spam calls, texts, and/or emails; (vi) nominal damages; (vii) emotional distress; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to take appropriate and adequate measures to protect their Private Information.

22. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach (the "Class").

23. Accordingly, Plaintiffs bring this action against Defendant for (i) negligence, (ii) breach of implied contract, (iii) unjust enrichment, (iv) breach of third-party beneficiary contract, (v) invasion of privacy, and (vi) declaratory relief, seeking redress for CPS's unlawful conduct.

24. Plaintiffs seek remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate, long term credit monitoring services funded by Defendant, and declaratory relief.

II. PARTIES

PLAINTIFFS

Plaintiff Patrick Dunn

25. Plaintiff Patrick Dunn (for this section, "Plaintiff") is and was at all times relevant to this Complaint an individual citizen of the State of Massachusetts, residing in the city of Walpole.

26. On or about February 25, 2025, Plaintiff received notice of the Breach via letter that his employer's employees had been victims of the Data Breach and that Defendant was preparing its response to the Data Breach. Plaintiff is employed by Cutler & Associates, a law firm that contracts with Defendant for payroll and human resources functions.

27. Shortly after and as a result of the Breach, Plaintiff began experiencing a drastic increase in spam phone calls and texts each month, including persistent efforts to get him to pay non-existent tickets allegedly from the Massachusetts State Police. Given that this spam is received via the same number that he provided to his employer, Plaintiff reasonably believes this spam is a result of the Breach.

28. In response to CPS's Notice of Data Breach, Plaintiff will be required to spend time dealing with the consequences of the Data Breach, including time spent verifying the legitimacy of the Notice Letter, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts.

29. As a result of the Data Breach and at the recommendation of Defendant, Plaintiff has spent approximately 10 hours dealing with the fallout from the Breach (including monitoring his credit and financial accounts) and he will continue to do so.

30. Plaintiff greatly values his privacy and Private Information. Plaintiff takes reasonable steps to maintain the confidentiality of his Private Information, *e.g.*, Plaintiff stores sensitive documents with Private Information in safe and secure locations and safely destroys sensitive documents; diligently selects unique usernames and passwords; and has not knowingly transmitted unencrypted Private Information over the internet or other unsecured sources.

31. Plaintiff would not have provided CPS with his Private Information had CPS disclosed that it lacked data security practices adequate to safeguard it.

32. Plaintiff suffered actual injury in the form of damages and diminution in the value of his Private Information—a form of intangible property that he entrusted to CPS (or its customer).

33. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number.

34. Plaintiff reasonably believes that the cybercriminals may have already sold his Private Information. Had Plaintiff been notified of CPS's Breach in a timelier manner, Plaintiff could have attempted to mitigate his injuries.

35. Plaintiff is at an imminent and impending risk of injury arising (specifically, the substantially increased risk of fraud, identity theft, and misuse) resulting from the theft and likely sale of Plaintiff's Private Information, including his Social Security number.

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

Plaintiff Patricia Brown

37. Plaintiff Patricia Brown (for this section, "Plaintiff") is and was at all times relevant to this Complaint an individual citizen of the State of Rhode Island, residing in the city of Cranston (Providence County).

38. Upon information and belief, Plaintiff's employee benefits are administered by CPS. Upon information and belief, Plaintiff's employer is a customer of CPS.

39. CPS required that either its customer or Plaintiff provide CPS with Plaintiff's Private Information. CPS was provided with Plaintiff's Private Information, including but not limited to Plaintiff's Social Security number.

40. On or about May 1, 2025, Plaintiff received a Notice Letter informing Plaintiff that her critical Private Information was accessed by an unauthorized actor. The letter stated that the extracted information included her "name, account number, and social security number," but did not expand on whether additional information was stolen as well.

41. Plaintiff is alarmed by the amount of her Personal Information that was stolen or accessed, and even more by the fact that her Social Security number was identified as among the breached data from CPS's computer systems.

42. Subsequent to and as a result of the Breach, Plaintiff was the victim of attempted fraud when she received multiple, fraudulent PayPal invoices regarding the purchase of Bitcoin and seeking additional information from her.

43. Shortly after and as a result of the Breach, Plaintiff began experiencing a drastic increase in the number of spam calls, texts, and emails per day she received. Given that this spam is received via the same number and email she provided to her employer, Plaintiff reasonably believes this spam is a result of the Breach. Plaintiff is concerned that the spam calls and texts are being placed with the intent of obtaining more personal information from her and committing identity theft by way of a social engineering attack.

44. Prior to the Data Breach, Plaintiff had never been a victim of fraud or attempted fraud.

45. In response to Defendant's Notice of Data Breach, Plaintiff will be required to spend time dealing with the consequences of the Data Breach, including time spent verifying the

legitimacy of the Notice of Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring her accounts.

46. As a result of the Data Breach and at the recommendation of Defendant, Plaintiff checked her financial accounts in an effort to mitigate the damage that CPS has caused and she will continue to do so.

47. Plaintiff greatly values her privacy and Private Information. Plaintiff takes reasonable steps to maintain the confidentiality of her Private Information, *e.g.*, Plaintiff stores sensitive documents with Private Information in safe and secure locations and safely destroys sensitive documents; diligently selects unique usernames and passwords; and has not knowingly transmitted unencrypted Private Information over the internet or other unsecured sources.

48. Plaintiff suffered actual injury and damages as a result of the Data Breach. Plaintiff would not have provided CPS with her Private Information had CPS disclosed that it lacked data security practices adequate to safeguard it.

49. Plaintiff suffered actual injury in the form of damages and diminution in the value of her Private Information—a form of intangible property that she entrusted to CPS (or its customer).

50. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy, especially her Social Security number.

51. Plaintiff reasonably believes that the cybercriminals may have already sold her Private Information. Had Plaintiff been notified of CPS's breach in a timelier manner, she could have attempted to mitigate her injuries.

52. Plaintiff is at an imminent and impending risk of injury arising (specifically, the substantially increased risk of fraud, identity theft, and misuse) resulting from the theft and likely sale of Plaintiff's Private Information, including her Social Security number.

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

Plaintiff Eric Marcial

54. Plaintiff Eric Marcial (for this section, "Plaintiff") is and was at all times relevant to this Complaint an individual citizen of the State of Maine, residing in the city of Blue Hill.

55. Upon information and belief, Plaintiff's employee benefits are administered by CPS. Upon information and belief, Plaintiff's employer is a customer of CPS.

56. CPS required that either its customer or Plaintiff provide CPS with Plaintiff's Private Information. CPS was provided with Plaintiff's Private Information, including but not limited to Plaintiff's Social Security number.

57. Plaintiff received the Notice Letter, by U.S. mail, directly from Defendant, dated April 25, 2025. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including his name and Social Security number.

58. As a result of the Data Breach and at Defendant's recommendation, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

59. Shortly after and as a result of the Breach, Plaintiff began experiencing an increase in spam calls, texts, and emails received. Given that this spam is received via the same number and email he provided to his employer, Plaintiff reasonably believes this spam is a result of the Breach. Plaintiff is concerned that the spam calls and texts are being placed with the intent of obtaining more personal information from him and committing identity theft by way of a social engineering attack.

60. Plaintiff greatly values his privacy and Private Information. Plaintiff takes reasonable steps to maintain the confidentiality of his Private Information, *e.g.*, Plaintiff stores sensitive documents with Private Information in safe and secure locations and safely destroys sensitive documents; diligently selects unique usernames and passwords; and has not knowingly transmitted unencrypted Private Information over the internet or other unsecured sources.

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

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

63. Plaintiff would not have provided Defendant with his Private Information had Defendant disclosed that it lacked data security practices adequate to safeguard it.

64. Plaintiff suffered actual injury in the form of damages and diminution in the value of his Private Information—a form of intangible property that he entrusted to CPS (or its customer).

65. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number.

66. Plaintiff reasonably believes that the cybercriminals may have already sold his Private Information. Had Plaintiff been notified of CPS's Breach in a timelier manner, Plaintiff could have attempted to mitigate his injuries.

67. Plaintiff is at an imminent and impending risk of injury arising (specifically, the substantially increased risk of fraud, identity theft, and misuse) resulting from the theft and likely sale of Plaintiff's Private Information, including his Social Security number.

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

Plaintiff Sokankelly Lim

69. Plaintiff Sokankelly Lim (for this section, "Plaintiff") is and was at all times relevant to this Complaint an individual citizen of the State of Massachusetts.

70. Some time prior to February 2024, Plaintiff obtained HR, benefits, and payroll services through an employer that utilizes the CPS network.

71. On or about April 25, 2025, Defendant sent Plaintiff a Notice Letter informing her that her critical Private Information was accessed by an unauthorized actor.

72. As a result of the Data Breach, Plaintiff suffered actual damages including, without limitation, lost time related to monitoring her financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of her personal information, and other economic and non-economic harm. Plaintiff will now be forced to expend additional

time, efforts, and potentially expenses to review her credit reports, monitor her financial accounts, and monitor for fraud or identify theft—particularly since the compromised information may include Social Security numbers.

73. As a result of the Data Breach and at the recommendation of Defendant, Plaintiff spent time reviewing her credit reports, reviewing various credit alerts received by text and email, checking her financial information, and dealing with increased spam text messages and emails, and she will continue to do so.

74. Shortly after and as a result of the Breach, Plaintiff received multiple notices from financial institutions that her Private Information had been found on the dark web.

75. Plaintiff has experienced anxiety and increased concerns arising from the fact that her Private Information has been or will be misused and from the loss of her privacy.

76. Plaintiff greatly values her privacy and Private Information. Plaintiff takes reasonable steps to maintain the confidentiality of her Private Information, *e.g.*, Plaintiff stores sensitive documents with Private Information in safe and secure locations and safely destroys sensitive documents; diligently selects unique usernames and passwords; and has not knowingly transmitted unencrypted Private Information over the internet or other unsecured sources.

77. Plaintiff would not have provided CPS with her Private Information had CPS disclosed that it lacked data security practices adequate to safeguard it.

78. Plaintiff suffered actual injury in the form of damages and diminution in the value of her Private Information—a form of intangible property that she entrusted to CPS (or its customer).

79. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy, especially her Social Security number.

80. Plaintiff reasonably believes that the cybercriminals may have already sold her Private Information. Had Plaintiff been notified of CPS's Breach in a timelier manner, Plaintiff could have attempted to mitigate her injuries.

81. Plaintiff is at an imminent and impending risk of injury arising (specifically, the substantially increased risk of fraud, identity theft, and misuse) resulting from the theft and likely sale of Plaintiff's Private Information, including her Social Security number.

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

Plaintiff Patrick Nowak

83. Plaintiff Patrick Nowak (for this section, "Plaintiff") is and was at all times relevant to this Complaint an individual citizen of the State of Florida, residing in the city of Tampa.

84. Upon information and belief, Plaintiff's employee benefits are administered by CPS. Upon information and belief, Plaintiff's former employer, Can Monkey, is a customer of CPS.

85. CPS required that either its customer or Plaintiff provide CPS with Plaintiff's Private Information. CPS was provided with Plaintiff's Private Information, including but not limited to Plaintiff's Social Security number.

86. On or about April 25, 2025, Defendant sent Plaintiff a Notice Letter informing Plaintiff that his critical Private Information was accessed by an unauthorized actor. The letter

stated that the extracted information included his "name, account number, and social security number," but did not expand on whether additional information was stolen as well.

87. Shortly after and as a result of the Breach, Plaintiff began experiencing an increase in spam calls, texts, and emails received. Given that this spam is received via the same number and email he provided to his employer, Plaintiff reasonably believes this spam is a result of the Breach. Plaintiff is concerned that the spam calls and texts are being placed with the intent of obtaining more personal information from his and committing identity theft by way of a social engineering attack.

88. As a result of the Data Breach and at the recommendation of Defendant, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach and reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. Plaintiff now monitors his financial and credit statements multiple times a week and has spent hours dealing with the Data Breach, valuable time he otherwise would have spent on work and recreation.

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

90. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress about his Private Information now being in the hands of cybercriminals, which has been compounded by the fact that Defendant still has not fully informed him of key details about the Data Breach or the exact data elements stolen. As an employee of Defendant's client, Plaintiff reasonably believes he is at a higher risk of fraud, and to suffer occupational and financial impact as a result of that fraud.

91. Plaintiff greatly values his privacy and Private Information. Plaintiff takes reasonable steps to maintain the confidentiality of his Private Information, *e.g.*, Plaintiff stores sensitive documents with Private Information in safe and secure locations and safely destroys sensitive documents; diligently selects unique usernames and passwords; and has not knowingly transmitted unencrypted Private Information over the internet or other unsecured sources.

92. Plaintiff would not have provided CPS with his Private Information had CPS disclosed that it lacked data security practices adequate to safeguard it.

93. Plaintiff suffered actual injury in the form of damages and diminution in the value of his Private Information—a form of intangible property that he entrusted to CPS (or its customer).

94. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number.

95. Plaintiff reasonably believes that the cybercriminals may have already sold his Private Information. Had Plaintiff been notified of CPS's Breach in a timelier manner, Plaintiff could have attempted to mitigate his injuries.

96. Plaintiff is at an imminent and impending risk of injury arising (specifically, the substantially increased risk of fraud, identity theft, and misuse) resulting from the theft and likely sale of Plaintiff's Private Information, including his Social Security number.

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

Plaintiff Carolyn Strycharz

98. Plaintiff Carolyn Strycharz (for this section, "Plaintiff") is and was at all times relevant to this Complaint an individual citizen of the State of Massachusetts.

99. Upon information and belief, Plaintiff's employee benefits are administered by CPS. Upon information and belief, Plaintiff's employer is a customer of CPS.

100. CPS required that either its customer or Plaintiff provide CPS with Plaintiff's Private Information. CPS was provided with Plaintiff's Private Information, including but not limited to Plaintiff's Social Security number.

101. On or about May 1, 2025, Plaintiff received a Notice Letter informing Plaintiff that her critical Private Information was accessed by an unauthorized actor. The letter stated that the extracted information included her "name, account number, and social security number," but did not expand on whether additional information was stolen as well.

102. As a result of the Data Breach and at the direction of Defendant's Notice Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring her financial accounts for any indication of fraudulent activity. Plaintiff has spent significant time on mitigation activities in response to the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

103. Shortly after and as a result of the Breach, Plaintiff was notified that her Private Information was found on the dark web.

104. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach.

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

106. Plaintiff greatly values her privacy and Private Information. Plaintiff takes reasonable steps to maintain the confidentiality of her Private Information, *e.g.*, Plaintiff stores sensitive documents with Private Information in safe and secure locations and safely destroys sensitive documents; diligently selects unique usernames and passwords; and has not knowingly transmitted unencrypted Private Information over the internet or other unsecured sources.

107. Plaintiff suffered actual injury and damages as a result of the Data Breach. Plaintiff would not have provided CPS with her Private Information had CPS disclosed that it lacked data security practices adequate to safeguard it.

108. Plaintiff suffered actual injury in the form of damages and diminution in the value of her Private Information—a form of intangible property that she entrusted to CPS (or its customer).

109. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy, especially her Social Security number.

110. Plaintiff reasonably believes that the cybercriminals may have already sold her Private Information. Had Plaintiff been notified of CPS's Breach in a timelier manner, Plaintiff could have attempted to mitigate her injuries.

111. Plaintiff is at an imminent and impending risk of injury arising (specifically, the substantially increased risk of fraud, identity theft, and misuse) resulting from the theft and likely sale of Plaintiff's Private Information, including her Social Security number.

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

Plaintiff James Connors

113. Plaintiff James Connors (for this section, "Plaintiff") is and was at all times relevant to this Complaint an individual citizen of the State of New York, residing in the city of Chappaqua.

114. Upon information and belief, Plaintiff's employee benefits are administered by CPS. Upon information and belief, Plaintiff's employer is a customer of CPS.

115. CPS required that either its customer or Plaintiff provide CPS with Plaintiff's Private Information. CPS was provided with Plaintiff's Private Information, including but not limited to Plaintiff's Social Security number.

116. On or about April 25, 2025, Defendant sent Plaintiff a Notice Letter informing Plaintiff that his critical Private Information was accessed by an unauthorized actor. The letter stated that the extracted information included his "name, account number, and social security number," but did not expand on whether additional information was stolen as well.

117. As a result of the Data Breach and at the recommendation of Defendant, Plaintiff has spent time and effort checking his accounts, verifying the legitimacy of the Data Breach Notice Letter, self-monitoring his own accounts and credit reports to ensure no additional fraudulent activity has occurred, and otherwise mitigating the harmful effects of the Data Breach. This time, which has been lost forever and cannot be recaptured, was incurred as a result of the Data Breach.

118. The substantial risk of imminent harm and loss of privacy resulting from the Data Breach have caused Plaintiff to suffer stress, fear, and anxiety, especially the indefinite prospect of Plaintiff's Private Information being available to third parties for the rest of his life.

119. Plaintiff greatly values his privacy and Private Information. Plaintiff takes reasonable steps to maintain the confidentiality of his Private Information, *e.g.*, Plaintiff stores sensitive documents with Private Information in safe and secure locations and safely destroys sensitive documents; diligently selects unique usernames and passwords; and has not knowingly transmitted unencrypted Private Information over the internet or other unsecured sources.

120. Plaintiff suffered actual injury and damages as a result of the Data Breach. Plaintiff would not have provided CPS with his Private Information had CPS disclosed that it lacked data security practices adequate to safeguard it.

121. Plaintiff suffered actual injury in the form of damages and diminution in the value of his Private Information—a form of intangible property that he entrusted to CPS (or its customer).

122. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number.

123. Plaintiff reasonably believes that the cybercriminals may have already sold his Private Information. Had Plaintiff been notified of CPS's Breach in a timelier manner, Plaintiff could have attempted to mitigate his injuries.

124. Plaintiff is at an imminent and impending risk of injury arising (specifically, the substantially increased risk of fraud, identity theft, and misuse) resulting from the theft and likely sale of Plaintiff's Private Information, including his Social Security number.

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

DEFENDANT

126. CPS is a Massachusetts limited liability company organized and headquartered in Springfield, Massachusetts. CPS's principal place of business is located at 1 Carando Drive, Springfield, Massachusetts 01104. Defendant can be served through its registered agent at: CT Corporation System, 115 Federal Street, Ste 700, Boston, Massachusetts 02110.

III. JURISDICTION AND VENUE

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

128. The Court has personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business or business venture in this State; it is registered with the Secretary of State as a limited liability company; it maintains its headquarters in Massachusetts; and committed tortious acts in Massachusetts.

129. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because it is the district within which CPS has the most significant contacts.

IV. STATEMENT OF FACTS

Nature of Defendant's Business.

130. CPS, founded in 2003, is a third-party administrator handling "human resource, benefits, and payroll service."[9]

131. CPS claims it has over 175 employees and over "10,000 clients across 50 states."[10]

[9] *About Us*, COMPLETE PAYROLL SOLUTIONS, https://www.completepayrollsolutions.com/about-us (last visited July 3, 2025).
[10] *Id.*

132. CPS, in the regular course of its business, collects and maintains the Private Information of clients' employees as a requirement of its business practices.

133. The customers of CPS provide their employees' and clients' Private Information to CPS with the mutual understanding that this highly sensitive private information was confidential and would be properly safeguarded from misuse and theft.

134. As a third-party payroll and benefits provider for small, medium, and large businesses, in addition to collecting PII, CPS collects and stores highly sensitive employee PHI. This PHI requires CPS to adhere to the laws, rules and regulations of HIPAA. CPS is aware of and publicly acknowledges its obligations on its website.[11]

135. CPS promises in it its Privacy Policy that "[a]ll of our systems are hosted in secure, hardened data centers to ensure safety and resilience against whatever the world throws at it."[12]

136. In the course of collecting Private Information from consumers, including Plaintiffs and Class Members, CPS promised to provide confidentiality and adequate security for Private Information through its applicable Privacy Policy and in compliance with statutory privacy requirements applicable to its industry. CPS is aware of and had obligations created by HIPAA, FTCA, contract, industry standards, and common law to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

137. CPS claims that "[w]e protect and secure your data and ensure compliance with industry standard regulations."[13]

[11] *Data Security & Privacy*, COMPLETE PAYROLL SOLUTIONS, https://www.completepayrollsolutions.com/data-security (last visited July 3, 2025).
[12] *Id.*
[13] *Id.*

138. Plaintiffs and the Class Members, as consumers, relied on the promises and duties of CPS to keep their sensitive Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

139. Consumers, in general, demand that businesses that require highly sensitive Private Information will provide security to safeguard their Private Information, especially when Social Security numbers and PHI are involved.

140. In the course of their dealings, Plaintiffs and Class Members provided CPS (either directly or through CPS's business customers) with the following types of Private Information:

- First and last names;
- Home addresses;
- Dates of birth;
- Financial information;
- HIPAA-protected information relating to medical history and health insurance;
- Photo identification and/or driver's licenses;
- Email addresses;
- Phone numbers; and
- Social Security numbers.

141. CPS had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure to third parties.

The Data Breach

142. According to its Notice Letters, on March 10, 2024, CPS "identified suspicious activity in its systems." After an unspecified amount of time (between the date they became aware

of the Breach and sent the Notice Letters), Defendant's investigation determined that an unauthorized actor accessed the CPS network and exfiltrated data therein.[14]

143. CPS did not begin providing Notice of the Breach to some victims until April 25, 2025, *over a year after the Breach began*. Therefore, *Plaintiffs' and Class Members' PII was in the hands of cybercriminals for over one year before they were notified* of CPS's Data Breach. Time is of the essence when trying to protect against identity theft after a data breach, so early notification is critical.

144. CPS reported to the Attorney General of Texas's website that the information breached contained names, addresses, Social Security numbers, driver's license numbers, financial information (*e.g.*, account number, credit or debit card number), and health insurance information.[15]

145. Because of this targeted, intentional cyberattack, data thieves were able to gain access to and obtain data from CPS that included the Private Information of Plaintiffs and Class Members.

146. Plaintiffs reasonably believe their stolen Private Information is currently available for sale on the dark web because that is the *modus operandi* of cybercriminals who target businesses that collect highly sensitive Private Information.[16]

---

[14] *Notice of Data Event*, COMPLETE PAYROLL SOLUTIONS, https://resources.completepayrollsolutions.com/hubfs/2025-announcements/cps-web-notification-event-20250310%5B87%5D.pdf?_gl=1*myls9d*_gcl_au*NDIxMjI0MTM3LjE3NDYwMjgwNjI.*_ga*Nzk1ODgxMDQ5LjE3NDYwMjgwNjI.*_ga_GJLNT3E4W0*MTc0NjIwODY5NS4yLjEuMTc0NjIwOTk5MS40OS4wLjA (last visited July 3, 2025).

[15] *Complete Payroll Solutions*, *Data Security Breach Reports*, ATT'Y GEN. OF TEX., *supra* note 1.

[16] *What is Multi-Extortion Ransomware?*, PALO ALTO NETWORKS, *supra* note 8.

147. Typically, in a ransomware attack, the criminal actor will not only encrypt the victim's system and block access until a ransom is paid but also exfiltrate data and threaten to release it to the dark web if a ransom is not paid. This scheme is known as a double-extortion attack. This scheme is used because many "organizations overcome the threat of file encryption with a simple up-to-date backup system."[17]

148. Meow, a well-known ransomware group, has taken responsibility for the Data Breach, publicly stating it accessed Defendant's information network and exfiltrated over three GB of data from Defendant's network related to at least 22,000 individuals.[18]

149. Meow, in fact, posted this data for sale on its leak site.[19]

[17] *Id.*
[18] *Complete Payroll Solutions notifies 22K+ people*, COMPARITECH, *supra* note 2.
[19] *Id.*

Price in one hands

16000$

Price in several hands

8000$

Description

Dear customers!

We are thrilled to offer an exclusive opportunity to access over 3 GB of confidential data from Complete Payroll Solutions (CPS), a leading provider of payroll, HR, and employee benefits services across the United States. Since its founding in 2003, CPS has grown to serve more than 10,000 clients nationwide, offering comprehensive workforce management solutions that include payroll processing, tax filing, talent management, benefits administration, and HR compliance.

CPS is known for its personalized approach, assigning dedicated account managers to ensure each client receives tailored support. The company integrates advanced technology into its services, streamlining payroll and HR tasks for efficiency and ease of use. CPSs offerings include paperless payroll, automated time tracking, compliance services, and more. They also assist with employee benefits management, including health insurance, retirement plans, and workers compensation.

With a mission to simplify workforce management, CPS remains a trusted partner across various industries. Headquartered in Springfield, Massachusetts, the company also operates additional offices across the northeastern United States.

This comprehensive 3 GB data pack includes:

Employee data
Client information
Scanned payment documents
Personal data (including dates of birth, social security numbers, and more)
Tax documents and payment records
And much more confidential information

These records offer in-depth insights into the companys operations, making them valuable to competitors, industry analysts, and other professionals.

To gain access to this exclusive dataset, simply click the Buy button and complete your registration. Our team will promptly reach out to ensure a smooth and confidential transaction process.

Dont miss out on the opportunity to explore detailed information from Complete Payroll Solutions with this comprehensive 3 GB data pack!

BUY

150. To prove its possession of the breached data, the Meow group posted sample images of documents stolen from CPS.[20]

[20] *Id.*


MEOW LEAKS
Search...
FEED
COMPLETE
PAYROLL SOLUTIONS

151. Meow states that the stolen data, which is now for sale, includes employee data, client information, scanned payment documents, personal data (including "dates of birth, social security numbers"), tax documents, payment records, and more.[21]

152. Upon information and belief, CPS failed to pay a ransom to Meow to secure CPS's breached data. As a result, Meow placed the Private Information of Plaintiffs and Class Members on the dark web for sale.

153. As a result of the Data Breach, CPS now belatedly encourages Class Members "to remain vigilant against incidents of identity theft and fraud and to review your accounts statements and credit reports to detect errors or suspicious activity" and to enroll in credit monitoring, fraud consultation, and identity theft restoration services, a tacit admission of the imminent risk of identity theft faced by Plaintiffs and Class Members, after waiting more than a year to send Notice Letters.[22]

154. That CPS is encouraging Plaintiffs and Class Members to enroll in credit monitoring and identity theft restoration services is an acknowledgment that the impacted consumers are subject to a substantial and imminent threat of fraud and identity theft.

155. CPS had obligations created by contract, industry standards, and common law to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

156. CPS could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their network and computer files containing PII.

157. Instead, Defendant failed to abide by its own Privacy Policy.

[21] *Id.*
[22] Notice Letter.

158. Defendant failed to adequately encrypt, redact, and protect Plaintiffs' and Class Members' Private Information.[23]

159. Defendant failed to maintain adequate intrusion detection and data exfiltration tools.[24]

160. Defendant failed to maintain adequate network access logs.[25]

161. Defendant failed to adequately train its employees and cybersecurity partners on cybersecurity policies and then fails to enforce those policies.[26]

162. Defendant was able to implement reasonable safeguards that would have prevented or mitigated the effects of the Data Breach but failed to do so.[27]

Defendant Acquires, Collects, and Stores Plaintiffs' and Class Members' Private Information.

163. By obtaining, collecting, and using Plaintiffs' and Class Members' Private Information for its own financial gain and business purposes, Defendant assumed legal and equitable duties and knew that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

---

[23] Notice Letter (admitting that "an unknown, unauthorized individual accessed and/or acquired certain information stored on CPS' systems").

[24] *See* https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/ece1a563-aa70-4247-b2b7-0fe1370174d5.html *with* Notice Letter (admitting that the Breach began on February 21, 2024, but was not discovered by Defendant until March 10, 2024, and likely was discovered by Defendant only after it received a ransom demand from the threat actor).

[25] Notice Letter (admitting that Defendant was unable to conclusively determine what exact Private Information was compromised and that after an investigation, Defendant was able to determine only that "the unauthorized individual likely accessed and or acquired [certain] information") (emphasis added).

[26] Ransomware attacks typically involve phishing attacks targeted at company employees in order to gain access to their user credentials. *See also* Notice Letter (admitting that after the Breach, Defendant decided it needed to "implement additional safeguards and training to its employees").

[27] Notice Letter (admitting that Defendant was able to "immediately" remediate the intrusion and block the vector of attack, *i.e.*, Defendant "reset system passwords [and] added extra layers of security").

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

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

The Data Breach Was a Foreseeable Risk of Which Defendant Was on Notice.

166. It is well known that Private Information, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of cybercriminals. Companies that collect such information, including CPS, are well aware of the risk of being targeted by cybercriminals.

167. Individuals place a high value not only on their Private Information, but also on the privacy of that data. Identity theft causes severe negative consequences to its victims, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

168. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are

not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss."[28]

169. Individuals, like Plaintiffs and Class Members, are particularly concerned with protecting the privacy of their Social Security numbers, which are the key to stealing any person's identity and is likened to accessing your DNA for hacker's purposes.

170. Data breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiffs and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse.

171. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[29]

172. In 2021, there were a record 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[30]

---

[28] "Victims of Identity Theft, 2018," U.S. DEP'T OF JUSTICE (Apr. 2021, NCJ 256085), https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last visited May 2, 2025).

[29] *Identity Theft and Your Social Security Number*, SSA (Oct. 2024), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 3, 2025).

[30] Bree Fowler, *Data breaches break record in 2021*, CNET (Jan. 24, 2022), https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last visited July 3, 2025).

173. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches since 2020. Over the next two years, in a poll done on security executives, they have predicted an increase in attacks from "social engineering and ransomware" as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[31]

174. In light of high profile data breaches at other industry leading companies, 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), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or should have known that its computer network would be targeted by cybercriminals.

175. 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, and prepared for, and hopefully can ward off a cyberattack.

176. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data." [32] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't

[31] Chuck Brooks, *Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know*, FORBES (June 3, 2022), https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last visited July 3, 2025).
[32] *Ransomware*, FBI, https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last visited July 3, 2025).

guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity."[33]

177. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep Private Information private and secure, CPS failed to take appropriate steps to protect the Private Information of Plaintiffs and the proposed Class from being compromised.

178. Defendant failed to abide by its own Privacy Policy.[34]

At All Relevant Times Defendant Had a Duty to Plaintiffs and Class Members to Properly Secure Their Private Information

179. At all relevant times, CPS had a duty to Plaintiffs and Class Members to properly secure their Private Information, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiffs and Class Members, and to promptly notify Plaintiffs and Class Members when CPS became aware that their Private Information was compromised.

180. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Defendant breached its common law, statutory, and other duties owed to Plaintiffs and Class Members.

181. Security standards commonly accepted among businesses that store Private Information using the internet include, without limitation:

[33] *Id.*
[34] *Data Security & Privacy*, COMPLETE PAYROLL SOLUTIONS, *supra* note 11.

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for Private Information;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

182. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[35] 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."[36]

183. The ramifications of Defendant's failure to keep consumers' Private Information secure are long lasting and severe. Once Private Information is stolen, particularly Social Security

[35] 17 C.F.R. § 248.201 (2013).
[36] *Id*.

and driver's license numbers, fraudulent use of that information and damage to victims including Plaintiffs and the Class may continue for years.

The Value of Personal Identifiable Information

184. The Private Information of consumers 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. For example, personal information can be sold at a price ranging from $40 to $200.[37]

185. Criminals can also purchase access to entire company's data breaches from $900 to $4,500.[38]

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

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[39]

187. Attempting to change or cancel a stolen Social Security number is difficult if not

[37] *Your personal data is for sale on the dark web. Here's how much it costs*, DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited July 3, 2025).
[38] *In the Dark*, VPNOVERVIEW (2019), https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited July 3, 2025).
[39] *Identity Theft and Your Social Security Number*, SSA, *supra* note 29.

nearly impossible. An individual cannot obtain a new Social Security number without evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

188. Even 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."[40]

189. 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."[41]

190. Private Information can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[42]

191. Given the nature of this Data Breach, it is foreseeable that the compromised Private Information can be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiffs' and Class Members' Private Information can easily

[40] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited July 3, 2025).
[41] 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 (last visited July 3, 2025).
[42] *See* Office of Mgmt. & Budget, *OMB Memorandum M-07-16* n.1 (last visited July 3, 2025).

obtain Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

192. The Private Information compromised in this Data Breach is static and difficult, if not impossible, to change (such as Social Security numbers).

193. Defendant has offered only a limited time subscription for identity theft monitoring. This limitation is inadequate where Defendant's victims are likely to face many years of identity theft.

194. Defendant's credit monitoring offer and advice to Plaintiffs and Class Members squarely places the burden on Plaintiffs and Class Members, rather than on the Defendant, to monitor and report suspicious activities to law enforcement. In other words, Defendant expects Plaintiffs and Class Members to protect themselves from its tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiffs and Class Members in credit monitoring services upon discovery of the Breach, Defendant merely sent instructions to Plaintiffs and Class Members about actions they can affirmatively take to protect themselves.

195. These services are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and they entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information.

196. The injuries to Plaintiffs and Class Members were directly and proximately caused by CPS's failure to implement or maintain adequate data security measures for the victims of its Data Breach.

Defendant Failed to Comply with FTC Guidelines

197. Federal and State governments have established security standards and issued

recommendations to mitigate the risk of data breaches and the resulting harm to consumers and financial institutions. The FTC has issued numerous guides for business highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[43]

198. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[44] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as 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 security problems.

199. The FTC emphasizes that early notification to data breach victims reduces injuries: "If you quickly notify people that their personal information has been compromised, they can take steps to reduce the chance that their information will be misused" and "thieves who have stolen names and Social Security numbers can use that information not only to sign up for new accounts in the victim's name, but also to commit tax identity theft. People who are notified early can take steps to limit the damage."[45]

200. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[46]

---

[43] *Start With Security*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited July 3, 2025).
[44] *Protecting Personal Information: A Guide for Business*, FTC, https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last visited July 3, 2025).
[45] *Data Breach Response: A Guide for Business*, FTC, https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business (last visited July 3, 2025).
[46] *See Start With Security*, FTC, *supra* note 43.

201. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to

allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

202. The FTC has brought enforcement actions against businesses for failing to protect consumer and consumer 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.

203. Because Class Members entrusted Defendant with their Private Information, Defendant had, and has, a duty to the Plaintiffs and Class Members to keep their Private Information secure.

204. Plaintiffs and the other Class Members reasonably expected that when they provide Private Information to Defendant (or to CPS's customers), Defendant would safeguard their Private Information.

205. CPS was at all times fully aware of its obligation to protect the personal and

financial data of consumers, including Plaintiffs and Members of the Class. CPS was also aware of the significant repercussions if it failed to do so. Its own Privacy Policies, quoted above, acknowledges this awareness.

206. CPS's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiffs' and Class Members' first names, last names, addresses, and Social Security numbers, and other highly sensitive and confidential information—constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Concrete Injuries Are Caused by Defendant's Inadequate Security.

207. Plaintiffs and Class Members reasonably expected that Defendant would provide adequate security protections for their Private Information, and Class Members provided Defendant with sensitive personal information, including their names, addresses, and Social Security numbers.

208. Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. Plaintiffs and other individuals whose Private Information was entrusted with Defendant understood and expected that, as part of that business relationship, they would receive data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received data security that was of a lesser value than what they reasonably expected. As such, Plaintiffs and the Class Members suffered pecuniary injury.

209. Cybercriminals intentionally attack and exfiltrate Private Information to exploit it. Thus, Class Members are now, and for the rest of their lives will be, at a heightened and substantial risk of identity theft. Plaintiffs have also incurred (and will continue to incur) damages in the form of, inter alia, loss of privacy and costs of engaging adequate credit monitoring and identity theft

protection services.

210. The cybercriminals who obtained the Class Members' Private Information may exploit the information they obtained by selling the data in so-called "dark markets" or on the "dark web." Having obtained these names, addresses, Social Security numbers, and other Private Information, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

- obtaining employment;
- obtaining a loan;
- applying for credit cards or spending money;
- filing false tax returns;
- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public document.

211. In addition, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

212. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiffs and the other Class Members have been deprived of the value of their Private Information, for which there is a well-established national and international market.

213. Furthermore, Private Information has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for fraudulent misuse of this information to be detected.

214. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data

Breach have also placed Plaintiffs and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach." Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[47] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' Private Information will do so at a later date or re-sell it.

215. As a result of the Data Breach, Plaintiffs and Class Members have already suffered injuries, and each are at risk of a substantial and imminent risk of future identity theft.

216. CPS admits that the "unauthorized individual likely accessed and or acquired information" on its computer systems. In other words, cybercriminals actually exfiltrated the Private Information that was accessed.[48]

Data Breaches Put Consumers at an Increased Risk of Fraud and Identify Thef.t

217. Data breaches such as the one experienced Plaintiffs and the Class are especially problematic because of the disruption they cause to the overall daily lives of victims affected by the attack.

218. In 2019, the United States Government Accountability Office released a report

[47] *The Consumer Data Insecurity Report: Examining The Data Breach- Identity Fraud Paradigm In Four Major Metropolitan Areas*, https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf (last accessed May 2, 2025).
[48] *See* Notice Letter, Ex. A.

addressing the steps consumers can take after a data breach.[49] Its appendix of steps consumers should consider, in extremely simplified terms, continues for five pages. In addition to explaining specific options and how they can help, one column of the chart explains the limitations of the consumers' options. *See* GAO chart of consumer recommendations, reproduced and attached as Exhibit B. It is clear from the GAO's recommendations that the steps Data Breach victims (like Plaintiffs and the Class) must take after a breach like Defendant's are both time consuming and of only limited and short-term effectiveness.

219. The FTC, like the GAO (*see* Exhibit B), recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[50]

220. Theft of Private Information is also gravely serious. Private Information is a valuable property right.[51]

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

---

[49] U.S. Gov't Accountability Off., GAO-19-230, *Data Breaches: Range of Consumer Risks Highlights Limitations of Identity Theft Services* (Mar. 2019), https://www.gao.gov/assets/gao-19-230.pdf (last visited July 3, 2025), attached as Ex. B.

[50] *See Identity Theft Checklist*, FTC, https://www.identitytheft.gov/Steps (last visited July 3, 2025).

[51] *See*, *e.g.,* John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3–4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

222. There is a strong probability that the entirety of the stolen information has been dumped on the black market or will be dumped on the black market, meaning Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members must vigilantly monitor their financial and medical accounts for many years to come.

223. As the HHS warns, "PHI can be exceptionally valuable when stolen and sold on a black market, as it often is. PHI, once acquired by an unauthorized individual, can be exploited via extortion, fraud, identity theft and data laundering. At least one study has identified the value of a PHI record at $1000 each."[52]

V. CLASS ACTION ALLEGATIONS

224. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated ("the Class").

225. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All individuals whose Private Information was maintained on Complete Payroll Solutions, LLC's computer systems and who were sent a Notice Letter.

226. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

227. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

---

[52] *A Cost Analysis of Healthcare Sector Data Breaches Health Sector Cybersecurity Coordination Center (HC3)* at 2, HHS (Apr. 12, 2019), https://www.hhs.gov/sites/default/files/cost-analysis-of-healthcare-sector-data-breaches.pdf (citations omitted) (last visited July 3, 2025).

228. Numerosity. The Class Members are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of approximately thousands of persons whose data was compromised in Data Breach. Defendant maintains records to show the number of Class Members.

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

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

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

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

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

e. Whether Defendant owed a duty to Plaintiffs and Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Plaintiffs and Class Members to safeguard their Private Information;

g. Whether computer hackers obtained Plaintiffs' and Class Members' Private Information in the Data Breach;

h. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

l. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

230. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach.

231. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

232. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' Private Information was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

233. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is

superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

234. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

a. Further, Plaintiffs and Class Members have an interest in ensuring that their Private Information (which is believed to remain in the possession of Defendant) is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, ensuring that their Private Information is not accessible online, is encrypted, and is password protected. Damages from a future breach due to Defendant's inadequate data security represent an irreparable injury (such as the further loss of privacy and exposure of Private Information) for which no adequate remedy at law exists.

b. Plaintiffs and Class Members also have an interest in being informed of the full extent to which their Private Information has been breached, including being informed of (i) each, specific data element of their Private Information exfiltrated in the Breach; (ii) the security deficiency exploited in the Breach; and (iii)

whether the security deficiency exploited in the Breach was previously exploited to exfiltrate Private Information pertaining to Plaintiffs and Class Members.

235. Particular issues under Fed. R. Civ. P. 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

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

b. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

c. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

d. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

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

236. Finally, all Members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice of the Data Breach by CPS.

VI. CAUSES OF ACTION

FIRST COUNT
Negligence
(On behalf of Plaintiffs and All Class Members)

237. Plaintiffs re-allege and incorporate by reference paragraphs 1–236 above as if fully

set forth herein.

238. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of the regular course of its business operations. Plaintiffs and Class Members were entirely dependent on Defendant to use reasonable measures to safeguard their Private Information and were vulnerable to the foreseeable harm described herein should Defendant fail to safeguard their Private Information.

239. By collecting and storing this data in its computer property, and sharing it, and using it for commercial gain, Defendant assumed a duty of care to use reasonable means to secure and safeguard their computer property—and Plaintiffs' and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

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

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

242. Plaintiffs and the Class are within the class of persons that the FTCA was intended to protect.

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

244. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of its business of soliciting its services to its clients and its clients' employees, which solicitations and services affect commerce.

245. Defendant violated the FTCA by failing to use reasonable measures to protect the Private Information of Plaintiffs and Class Members and by not complying with applicable industry standards, as described herein.

246. Defendant breached its duties to Plaintiffs and Class Members under the FTCA by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiffs' and Class Members' Private Information, and by failing to provide prompt notice without reasonable delay.

247. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and those who received its services, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiffs and Class Members from a data breach.

248. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the

healthcare, medical, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

249. Defendant's multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

250. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

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

252. 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 Private Information that was in Defendant's possession.

253. Defendant was in a special relationship with Plaintiffs and Class Members with respect to the breached information because the aim of Defendant's data security measures was to benefit Plaintiffs and Class Members by ensuring that their personal information would remain protected and secure. Only Defendant was in a position to ensure that its systems were sufficiently secure to protect Plaintiffs' and Class Members' Private Information. The harm to Plaintiffs and Class Members from its exposure was highly foreseeable to Defendant.

254. 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 Private Information, including taking action to reasonably 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.

255. 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.

256. Defendant had duties to protect and safeguard the Private Information of Plaintiffs and the Class from being vulnerable to compromise by taking common-sense precautions when dealing with sensitive Private Information. 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' Private Information was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiffs' and Class Members' Private Information in its 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 Private Information.

257. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Private Information that had been entrusted to them.

258. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and Class Members' Private Information. Defendant breached its duties by, among other things:

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

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

c. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information;

d. Failing to adequately train its employees to not store unencrypted Private Information 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 Class Members' Private Information;

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 Plaintiffs and Class Members of the Data Breach that affected their Private Information.

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

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

261. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Private Information 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 Private Information of Plaintiffs and Class Members while it was within Defendant's possession and control.

262. 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 securing their Private Information and mitigating damages.

263. 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 Private Information, and closely reviewing and monitoring bank accounts, credit reports, and statements sent from providers and their insurance companies.

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

265. 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 grossly negligent conduct.

266. Plaintiffs and the Class have suffered injury and are entitled to actual damages in amounts to be proven at trial.

SECOND COUNT
Breach of Implied Contract
(On Behalf of Plaintiffs and All Class Members)

267. Plaintiffs re-allege and incorporate by reference paragraphs 1–236 above as if fully set forth herein.

268. Plaintiffs and Class Members were required to provide their Private Information to

Defendant as a condition of receiving services provided by Defendant.

269. Plaintiffs and Class Members provided their Private Information to Defendant or its third-party agents in exchange for CPS's services or employment. In exchange for the Private Information, Defendant promised to protect their Private Information from unauthorized disclosure.

270. At all relevant times Defendant promulgated, adopted, and implemented written a Privacy Policy and HIPAA Notice whereby it expressly promised Plaintiffs and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

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

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

273. When Plaintiffs and Class Members provided their Private Information to Defendant as a condition of relationship, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

274. Defendant required Class Members to provide their Private Information as part of Defendant's regular business practices.

275. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

276. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

277. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

278. Defendant breached its implied contracts with Plaintiffs and Class Members by failing to safeguard and protect their Private Information.

279. As a direct and proximate result of Defendant's breaches of the implied contracts, Class Members sustained damages as alleged herein.

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

281. Plaintiffs and Class Members are also entitled to nominal damages for the breach of implied contract.

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

adequate long term credit monitoring to all Class Members for a period longer than the grossly inadequate one-year currently offered.

THIRD COUNT
Breach Of Third-Party Beneficiary Contract
(On Behalf of Plaintiffs and Class Members)

283. Plaintiffs re-allege and incorporate by reference paragraphs 1–236 above as if fully set forth herein.

284. Upon information and belief, Defendant entered into virtually identical contracts with its clients to provide employee payroll and benefit services, which included providing data security practice, procedures, and protocols sufficient to safeguard the Private Information that was to be entrusted to it.

285. Such contracts were made expressly for the benefit of Plaintiffs and the Class, as it was their Private Information that Defendant agreed to receive and protect through its services. Thus, the benefit of collection and protection of the Private Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties, and Plaintiffs and Class Members were direct and express beneficiaries of such contracts.

286. Defendant knew that if it were to breach these contracts with its clients, Plaintiffs and the Class would be harmed.

287. Defendant breached its contracts with its clients and, as a result, Plaintiffs and Class Members were harmed by this Data Breach when Defendant failed to use reasonable data security and/or business associate monitoring measures that could have prevented the Data Breach.

288. As foreseen, Plaintiffs and Class Members were harmed by Defendant's failure to use reasonable data security measures to securely store Plaintiffs' and Class Members' Private Information. Such harms include, but are not limited to, the immediate and substantial risk of harm through the loss of their Private Information.

289. Accordingly, Plaintiffs and the Class are entitled to actual damages and nominal in the amount to be determined at trial, along with costs and attorneys' fees incurred in this action.

FOURTH COUNT
Invasion Of Privacy/Intrusion Upon Seclusion
(On behalf of Plaintiff and Class Members)

290. Plaintiffs re-allege and incorporate by reference paragraphs 1–236 above as if fully set forth herein.

291. Plaintiffs and Class Members had a legitimate expectation of privacy in their Private Information in Defendant's possession and were entitled to Defendant's protection of this Private Information against disclosure to unauthorized third parties.

292. Defendant owed a duty to its clients' employees, including Plaintiffs and Class Members, to keep their Private Information confidential and secure.

293. Defendant failed to protect Plaintiffs' and Class Members' Private Information and instead exposed it to unauthorized persons, criminal hackers, which on information and belief have made or imminently will make the Private Information publicly available and disseminated it to thousands of people, including through publishing the data on dark web leak sites, where cybercriminals go to find their next identity theft and extortion victims.

294. Defendant allowed unauthorized third parties access to and examination of the Private Information of Plaintiffs and Class Members, by way of Defendant's failure to protect the Private Information through reasonable data security measures.

295. The unauthorized release to, custody of, and examination by unauthorized third parties of the Private Information of Plaintiffs and Class Members is highly offensive to a reasonable person and represents an intrusion upon Plaintiffs' and Class Members' seclusion as well as a public disclosure of private facts.

296. The intrusion was into a place or thing, which was private and is entitled to be

private.

297. Plaintiffs and Class Members disclosed their Private Information to Defendant (directly or indirectly) as a condition of and in exchange for receiving services, including that their Private Information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and not be disclosed without their authorization, given Defendant's promises to that effect.

298. Subsequent to the intrusion, Defendant permitted Plaintiffs' and Class Members' data to be accessed by hackers and, imminently if not already, published online to countless cybercriminals whose mission is to misuse such information through fraud and extortion.

299. The Data Breach constitutes an intentional or reckless interference by Defendant of Plaintiffs' and Class Members' interests in solitude or seclusion, as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

300. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it had actual knowledge that its information security practices were insufficient to protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

301. Defendant acted with reckless disregard for Plaintiffs' and Class Members' privacy when it allowed improper access to its systems containing Plaintiffs' and Class Members' Private Information without protecting said data from the unauthorized disclosure, or even encrypting it.

302. Defendant was aware of the potential of a data breach but failed to adequately safeguard its network systems or implement appropriate policies to prevent the unauthorized release of Plaintiffs' and Class Members' Private Information to cybercriminals.

303. Because Defendant acted with this knowing state of mind, it had notice and knew that its inadequate and insufficient information security practices would cause injury and harm to

Plaintiffs and Class Members.

304. As a direct and proximate result of Defendant's acts and omissions set forth above, Plaintiffs' and Class Members' Private Information was disclosed to third parties without authorization, causing Plaintiffs and Class Members to suffer injuries and damages including, without limitation, (a) invasion of privacy; (b) lost or diminished value of their Private Information; (c) out-of-pocket and lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) emotional distress due to their Private Information's publication on the dark web; and (e) the continued and certainly increased risk to their Private Information, which remains in Defendant's possession in unencrypted form and subject to further unauthorized disclosures, so long as Defendant fails to undertake appropriate and adequate measures to protect it.

305. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the Private Information maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and Class Members.

FIFTH COUNT
Unjust Enrichment
(On Behalf of Plaintiffs and All Class Members)

306. Plaintiffs re-allege and incorporate by reference paragraphs 1–236 above as if fully set forth herein.

307. This claim is plead in the alternative to the implied contract and third-party beneficiary contract claims.

308. Plaintiffs and Class Members conferred a monetary benefit on Defendant in the

form of the provision of their Private Information and Defendant would be unable to engage in its regular course of business without that Private Information.

309. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiffs and Class Members and accepted that monetary benefit.

310. However, acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

311. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures.

312. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

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

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

315. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered or will suffer injury, including but not limited to: (i) actual identity theft;

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

316. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

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

SIXTH COUNT
Declaratory Judgment
(On Behalf of Plaintiffs and All Class Members)

318. Plaintiffs re-allege and incorporate by reference paragraphs 1–236 above as if fully set forth herein.

319. 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. Furthermore, 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.

320. An actual controversy has arisen in the wake of Defendant's Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Private Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their Private Information.

321. Plaintiffs allege that Defendant's data security measures remain inadequate. Plaintiffs will continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

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

a. CPS continues to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, HIPAA, Section 5 of the FTCA, and various state statutes; and

b. CPS continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

323. The Court also should issue corresponding prospective injunctive relief requiring CPS to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information.

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

and Class Members 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.

325. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to CPS if an injunction is issued. Among other things, if another massive data breach occurs at CPS, Plaintiffs and Class Members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to CPS of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and CPS has a pre-existing legal obligation to employ such measures.

326. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at CPS, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose Private Information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class;

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

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to

disclose with specificity the type of Private Information compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

E. For declaratory relief as requested;

F. Ordering Defendant to pay for lifetime credit monitoring services for Plaintiffs and the Class;

G. For an award of actual damages, compensatory damages, and statutory damages, in an amount to be determined, as allowable by law;

H. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

I. Pre- and post-judgment interest on any amounts awarded; and

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

VIII. JURY TRIAL DEMANDED

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

Dated: July 3, 2025

Respectfully submitted,

/s/ Danielle L. Perry

Danielle L. Perry*
MASON LLP
5335 Wisconsin Avenue NW, Suite 640
Washington, DC 20015
Tel: (202) 429-2290
dperry@masonllp.com

Carl V. Malmstrom*
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
111 W. Jackson Blvd., Suite 1700

Chicago, Illinois 60604
Tel: (312) 984-0000
Fax: (212) 686-0114
malmstrom@whafh.com

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Ave., NW, Suite 440
Washington, DC 20015
Tel: 866.252.0878
dlietz@milberg.com

Interim Co-Lead Counsel for Plaintiffs

**Pro hac vice*