UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

IN RE: DISA GLOBAL DATA BREACH LITIGATION	Case No. 4:25-cv-00821 **CONSOLIDATED CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs Christopher Duiker, Jeffrey Bachman, Zenitra Crawford, Richard Rosenblum, Edward Chappell, and Patricio Castro (collectively "Plaintiffs"), through their attorneys, as individuals and on behalf of all others similarly situated, bring this Class Action Complaint against Defendant DISA Global Solutions, Inc. ("DISA" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiffs allege the following on information and belief—except as to their own actions, counsel's investigations, and facts of public record.

NATURE OF ACTION

1. This class action arises from Defendant's failure to protect highly sensitive data.

2. Defendant is a Texas-based company that provides "full-service employee screening solutions" including drug and alcohol testing, background screening, occupational medicine and testing, safety training and transportation compliance.[1]

[1] Overview, DISA LinkedIn, https://www.linkedin.com/company/disa-global-solutions/about/ (last visited June 13, 2025).

3. As such, Defendant stores a litany of highly sensitive personal identifiable information ("PII") about its customers' current, former, and prospective employees. But Defendant lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

4. Between February 9, 2024 and April 22, 2024—for *more than ten weeks*—cybercriminals had access to Defendant's network before the breach was discovered. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to the PII that Defendant maintained.

5. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's PII. In short, Defendant's failures placed the Class's PII in a vulnerable position—rendering them easy targets for cybercriminals.

6. Plaintiffs are Data Breach victims, having received a breach notice. Plaintiffs bring this class action on behalf of themselves, and all others harmed by Defendant's misconduct.

7. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before this Data Breach, individuals' private information was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

PARTIES

8. Plaintiff, Christopher Duiker, is natural person and citizen of Texas. He resides in Austin, Texas, where he intends to remain.

9. Plaintiff, Jeffrey Bachman, is natural person and citizen of Florida. He resides in St. Johns, Florida, where he intends to remain.

10. Plaintiff, Zenitra Crawford, is natural person and citizen of Nevada. She resides in Las Vegas, Nevada, where she intends to remain.

11. Plaintiff, Richard Rosenblum, is a natural person and citizen of Massachusetts. He resides in Boston, Massachusetts, where he intends to remain.

12. Plaintiff, Edward Chappell, is a natural person and citizen of Georgia. He resides in Marrieta, Georgia, where he intends to remain.

13. Plaintiff, Patricio Castro, is a natural person and citizen of California. He resides in Riverside, California, where he intends to remain.

14. Defendant, DISA Global Solutions, Inc., is a for-profit corporation incorporated under the laws of Delaware with its principal place of business at 12600 Northborough Drive, Suite 300, Houston, TX 77067.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Plaintiffs and Defendant are citizens of different states. And there are over 100 putative Class members.

16. This Court has personal jurisdiction over Defendant because it is headquartered in Texas, regularly conducts business in Texas, and has sufficient minimum contacts in Texas.

17. Venue is proper in this Court because Defendant's principal office is in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiffs' claims occurred in this District.

BACKGROUND

Defendant Collected and Stored the PII of Plaintiffs and the Class

18. Defendant has been providing employee screening services to over 55,000 customers throughout the U.S. and Canada since 1986.[2]

19. As part of its business, Defendant receives and maintains the PII of thousands of its customers' current, former, and prospective employees. In doing so, Defendant implicitly promises to safeguard their PII. After all, Plaintiffs and Class members themselves took reasonable steps to secure their PII.

20. In collecting and maintaining the Private Information, Defendant agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiffs and Class members themselves took reasonable steps to secure their Private Information.

21. Under state and federal law, businesses like Defendant have duties to protect their customers' current, former, and prospective employees' PII and to notify them about breaches.

22. Defendant recognizes these duties, declaring in its "Privacy Policy" that:

a. "Protecting your privacy is important to DISA Global Solutions, Inc. ("DISA");"

b. "All personal information will be transmitted and stored in a secure manner in accordance with the terms of this policy as DISA has taken measures to protect personal and confidential data;"

c. "DISA respects the privacy of the individuals and clients who are the subjects of DISA Services, including but not limited to background checks.

[2] *About*, DISA, https://disa.com/disa-difference (last visited June 13, 2025).

DISA will collect, store, and use confidential information following best practices and also in compliance with applicable law, including the FCRA;"

d. "We seek to use reasonable organizational, technical, and administrative measures to protect Personal Information under our control."[3]

Defendant's Data Breach

23. On April 22, 2024, Defendant discovered that an unauthorized actor had accessed its systems.[4]

24. Defendant's investigation revealed that "an unauthorized third party accessed [its] environment between February 9, 2024, and April 22, 2024."[5]

25. Thus, for over *ten weeks*, cybercriminals had unfettered access to Defendant's systems. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to the PII of its customers' current, former, and prospective employees.

26. Concerningly, Defendant admitted that the unauthorized actor not only accessed its systems, but actually "procured some information."[6]

27. Indeed, Defendant recognized the threat posed by cybercriminals acquiring this PII, stating that it "took measures to dissuade the threat actor from publicly releasing any acquired data and to provide confirmation of the deletion of the data."[7] This is further evidence that the PII is in

[3] Privacy Policy, DISA, https://disa.com/privacy-policy (last visited June 13, 2025).
[4] Exhibit A contains all of a copy of Disa's Notice Letter.
[5] *Id*.
[6] *Id*.
[7] DISA Incident: Update on Review of 'Potentially Affected Files' and Notification Plan, DataBreaches.Net, https://databreaches.net/2025/02/03/disa-incident-update-on-review-of-potentially-affected-files-and-notification-plan/, (last visited June 13, 2025).

the possession of cybercriminals, which puts Plaintiffs and Class Members at a continuing risk of identity theft and fraud.

28. Because of Defendant's Data Breach, at least the following types of PII were compromised:

a. names,

b. Social Security numbers,

c. driver's license numbers or state identification card numbers,

d. dates of birth, and/or

e. drug testing information.[8]

29. And yet, Defendant waited until February 21, 2025—*over an entire year* after the Data Breach began—before it began notifying the class.[9]

30. Thus, Defendant kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

31. And when Defendant did notify Plaintiffs and the Class of the Data Breach, Defendant acknowledged that their Data Breach created a present, continuing, and significant risk of suffering identity theft, warning Plaintiffs and the Class to "remain vigilant against the potential for identity theft and fraud and to monitor your credit reports for any suspicious activity."[10]

32. Defendant failed its duties when its inadequate security practices caused the Data Breach. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII. And thus, Defendant caused widespread injury and monetary damages.

---

[8] *Id.*
[9] Exhibit A.
[10] *Id.*

33. On information and belief, Defendant failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

34. Since the breach, Defendant "implemented additional security measures."[11] But this is too little too late. Simply put, these measures—which Defendant now recognizes as necessary—should have been implemented *before* the Data Breach.

35. Defendant has done little to remedy its Data Breach. True, Defendant has offered some victims credit monitoring and identity-related services.[12] But upon information and belief, such services are wholly insufficient to compensate Plaintiffs and Class members for the injuries that Defendant inflicted upon them.

36. Because of Defendant's Data Breach, the sensitive PII of Plaintiffs and Class members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiffs and Class members.

Plaintiff Duiker's Experience

37. Plaintiff Christopher Duiker is a consumer of Defendant's services. As a condition of his employment, Plaintiff was required to indirectly supply Defendant with his Private Information, including his name, contact information, Social Security number, and other sensitive information, by providing his Private Information to his employer or prospective employer for employment screening services to be performed by Defendant.

38. Plaintiff Duiker is a Data Breach victim, having received a Breach Notice in or around February 2025.[13]

---

[11] *Id*.
[12] *Id*.
[13] *Id*.

39. Thus, Defendant obtained and maintained Plaintiff Duiker's PII. And as a result, Plaintiff Duiker was injured by Defendant's Data Breach.

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

41. As a result of the Data Breach, Plaintiff Duiker made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, reviewing credit monitoring and identity theft protection services and monitoring financial accounts for any unusual activity, which may take years to detect. Plaintiff Duiker has spent significant time dealing with the Data Breach – valuable time he 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.

42. Plaintiff Duiker (or his current, former, or prospective employers) provided his PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Duiker's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

43. Through the Data Breach, Defendant exposed at least Plaintiff Duiker's name, Social Security number, and driver's license or state identification number.

44. Plaintiff Duiker has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff Duiker to take those steps in its breach notice.

45. Plaintiff Duiker fears for his personal financial security and worries about what information was exposed in the Data Breach.

46. Because of Defendant's Data Breach, Plaintiff Duiker has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Duiker's injuries are precisely the type of injuries that the law contemplates and addresses.

47. Plaintiff Duiker suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

48. Plaintiff Duiker suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

49. Plaintiff Duiker suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Duiker's PII right in the hands of criminals.

50. In addition, following the Data Breach, Plaintiff Duiker has experienced an increase in spam calls, texts, and/or email messages.

51. Because of the Data Breach, Plaintiff Duiker anticipates spending considerable amounts of time and money to try and mitigate his injuries.

52. Today, Plaintiff Duiker has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Bachman's Experience

53. Plaintiff Jeffrey Bachman is a consumer of Defendant's services. As a condition of his employment, Plaintiff Bachman was required to indirectly supply Defendant with his Private Information, including his name, contact information, Social Security number, and other sensitive information, by providing his Private Information to his employer or prospective employer for employment screening services to be performed by Defendant.

54. Plaintiff Bachman is a Data Breach victim, having received a Breach Notice in or around February 2025.

55. Thus, Defendant obtained and maintained Plaintiff's PII. And as a result, Plaintiff Bachman was injured by Defendant's Data Breach.

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

57. As a result of the Data Breach, Plaintiff Bachman made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, reviewing credit monitoring and identity theft protection services and monitoring financial accounts for any unusual activity, which may take years to detect. Plaintiff Bachman has

spent significant time dealing with the Data Breach – valuable time he 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.

58. Plaintiff Bachman (or his current, former, or prospective employers) provided his PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Bachman's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

59. Through the Data Breach, Defendant exposed at least Plaintiff Bachman's name and Social Security number.

60. Plaintiff Bachman has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff Bachman to take those steps in its breach notice.

61. Plaintiff Bachman fears for his personal financial security and worries about what information was exposed in the Data Breach.

62. Because of Defendant's Data Breach, Plaintiff Bachman has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Bachman's injuries are precisely the type of injuries that the law contemplates and addresses.

63. Plaintiff Bachman suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

64. Plaintiff Bachman suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

65. Plaintiff Bachman suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Bachman's PII right in the hands of criminals.

66. Indeed, following the Data Breach, Plaintiff Bachman was charged an account fee when an unauthorized actor fraudulently opened a Destiny Mastercard account in Plaintiff Bachman's name.

67. Because of the Data Breach, Plaintiff Bachman anticipates spending considerable amounts of time and money to try and mitigate his injuries.

68. Today, Plaintiff Bachman has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Crawford's Experience

69. Plaintiff Zenitra Crawford is a consumer of Defendant's services. As a condition of her employment, Plaintiff Crawford was required to indirectly supply Defendant with her Private Information, including her name, contact information, Social Security number, and other sensitive information, by providing her Private Information to her employer or prospective employer for employment screening services to be performed by Defendant.

70. Plaintiff Crawford is a Data Breach victim, having received a Breach Notice in or around February 2025.

71. Thus, Defendant obtained and maintained Plaintiff Crawford's PII. And as a result, Plaintiff Crawford was injured by Defendant's Data Breach.

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

73. As a result of the Data Breach, Plaintiff Crawford made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, reviewing credit monitoring and identity theft protection services and monitoring financial accounts for any unusual activity, which may take years to detect. Plaintiff Crawford has spent significant time dealing with the Data Breach – valuable time she 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.

74. Plaintiff Crawford (or her current, former, or prospective employers) provided her PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Crawford's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

75. Through the Data Breach, Defendant exposed at least Plaintiff Crawford's name, email address, phone number, Social Security number, government identification, and/or unique identifiers to associate individuals with DISA.

76. Plaintiff Crawford has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed Plaintiff Crawford to take those steps in its breach notice.

77. Plaintiff Crawford fears for her personal financial security and worries about what information was exposed in the Data Breach.

78. Because of Defendant's Data Breach, Plaintiff Crawford has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Crawford's injuries are precisely the type of injuries that the law contemplates and addresses.

79. Plaintiff Crawford suffered actual injury from the exposure and theft of her PII—which violates her rights to privacy.

80. Plaintiff Crawford suffered actual injury in the form of damages to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

81. Plaintiff Crawford suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Crawford's PII right in the hands of criminals.

82. In addition, following the Data Breach, Plaintiff Crawford has experienced an increase in spam calls, texts, and/or email messages.

83. Because of the Data Breach, Plaintiff Crawford anticipates spending considerable amounts of time and money to try and mitigate her injuries.

84. Today, Plaintiff Crawford has a continuing interest in ensuring that her PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Rosenblum's Experience

85. Plaintiff Richard Rosenblum is a consumer of Defendant's services. As a condition of his employment, Plaintiff Rosenblum was required to indirectly supply Defendant with his Private Information, including his name, contact information, Social Security number, and other sensitive information, by providing his Private Information to his employer or prospective employer for employment screening services to be performed by Defendant.

86. Plaintiff Rosenblum is a Data Breach victim, having received a Breach Notice in or around February 2025.

87. Thus, Defendant obtained and maintained Plaintiff Rosenblum's PII. And as a result, Plaintiff Rosenblum was injured by Defendant's Data Breach.

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

89. As a result of the Data Breach, Plaintiff Rosenblum made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, reviewing credit monitoring and identity theft protection services and monitoring financial accounts for any unusual activity, which may take years to detect. Plaintiff Rosenblum

has spent significant time dealing with the Data Breach – valuable time he 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.

90. Plaintiff Rosenblum (or his current, former, or prospective employers) provided his PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Rosenblum's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

91. Through the Data Breach, Defendant exposed at least Plaintiff Rosenblum's name and Social Security number.

92. Plaintiff Rosenblum has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff Rosenblum to take those steps in its breach notice.

93. Plaintiff Rosenblum fears for his personal financial security and worries about what information was exposed in the Data Breach.

94. Because of Defendant's Data Breach, Plaintiff Rosenblum has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Rosenblum's injuries are precisely the type of injuries that the law contemplates and addresses.

95. Plaintiff Rosenblum suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

96. Plaintiff Rosenblum suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

97. Plaintiff Rosenblum suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Rosenblum's PII right in the hands of criminals.

98. In fact, Plaintiff Rosenblum has received numerous notification that his information has been found on the dark web.

99. In addition, following the Data Breach, Plaintiff Rosenblum has experienced an increase in spam calls, texts, and/or email messages, as well as numerous alerts that his information was found on the dark web.

100. Because of the Data Breach, Plaintiff Rosenblum anticipates spending considerable amounts of time and money to try and mitigate his injuries.

101. Today, Plaintiff Rosenblum has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Chappell's Experience

102. Plaintiff Edward Chappell is a consumer of Defendant's services. As a condition of his employment, Plaintiff was required to indirectly supply Defendant with his Private Information, including his name, contact information, Social Security number, and other sensitive information, by providing his Private Information to his employer or prospective employer for employment screening services to be performed by Defendant.

103. Plaintiff is a Data Breach victim, having received a Breach Notice dated February 21, 2025.

104. Thus, Defendant obtained and maintained Plaintiff's PII. And as a result, Plaintiff was injured by Defendant's Data Breach.

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

106. As a result of the Data Breach, Plaintiff Rosenblum made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, reviewing credit monitoring and identity theft protection services and monitoring financial accounts for any unusual activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach – valuable time he 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.

107. Plaintiff (or his current, former, or prospective employers) provided his PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

108. Through the Data Breach, Defendant exposed at least Plaintiff's name and Social Security number.

109. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

110. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach.

111. Indeed, within a few months after the Data Breach, Plaintiff experienced two unauthorized fraudulent charges to his bank account.

112. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

113. Plaintiff suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

114. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

115. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Rosenblum's PII right in the hands of criminals.

116. In addition, following the Data Breach, Plaintiff has experienced a significant increase in spam calls, texts, and/or email messages, to the point that Plaintiff began working on changing his phone number and email address, as they were almost unusable due to the influx in spam.

117. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

118. Today, Plaintiff has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Castro's Experience

119. Plaintiff Patricio Castro is a consumer of Defendant's services. As a condition of his employment, Plaintiff was required to indirectly supply Defendant with his Private Information, including his name, contact information, Social Security number, and other sensitive information, by providing his Private Information to his employer or prospective employer for employment screening services to be performed by Defendant.

120. Plaintiff is a Data Breach victim, having received a Breach Notice dated February 21, 2025.

121. Thus, Defendant obtained and maintained Plaintiff's PII. And as a result, Plaintiff was injured by Defendant's Data Breach.

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

123. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach, reviewing credit monitoring and identity theft protection services and monitoring financial

accounts for any unusual activity, which may take years to detect. Plaintiff has spent significant time dealing with the Data Breach – valuable time he 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.

124. Plaintiff (or his current, former, or prospective employers) provided his PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

125. Through the Data Breach, Defendant exposed at least Plaintiff's name and Social Security number.

126. Plaintiff has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff to take those steps in its breach notice.

127. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach.

128. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

129. Plaintiff suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

130. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

131. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Rosenblum's PII right in the hands of criminals.

132. In addition, following the Data Breach, Plaintiff has experienced a significant increase in spam calls, texts, and/or email messages.

133. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

134. Today, Plaintiff has a continuing interest in ensuring that his PII—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

135. Because of Defendant's failure to prevent the Data Breach, Plaintiffs and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII is used;

b. diminution in value of their PII;

c. compromise and continuing publication of their PII;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII; and

h. continued risk to their PII—which remains in Defendant's possession—and is thus as risk for futures breaches so long as Defendant fails to take appropriate measures to protect the PII.

136. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

137. The value of Plaintiffs' and Class's PII on the black market is considerable. Stolen PII trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the "dark web"—further exposing the information.

138. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the PII far and wide.

139. One way that criminals profit from stolen PII is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen PII, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

140. The development of "Fullz" packages means that the PII exposed in the Data Breach can easily be linked to data of Plaintiffs and the Class that is available on the internet.

141. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and Class members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class members' stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

142. Defendant disclosed the PII of Plaintiffs and Class members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiffs and Class members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

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

Defendant Knew—Or Should Have Known—of the Risk of a Data Breach

144. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and or data breaches in recent years.

145. It is well known that PII, including Social Security numbers, is an invaluable commodity and a frequent target of hackers.

146. 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.[14]

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

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

149. 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, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

150. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks, including ransomware attacks involving data theft, because warnings were readily available and accessible via the internet.

151. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that,

[14] Data breaches break record in 2021, CNET (Jan. 24, 2022), https://www.cnet.com/news/privacy/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed June 13, 2025).

among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[15]

152. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[16]

153. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[17]

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

155. In light of the information readily available and accessible on the internet before

---

[15] High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations, FBI, available at https://www.ic3.gov/Media/Y2019/PSA191002 (last accessed June 13, 2025).

[16] Ransomware mentioned in 1,000+ SEC filings over the past year, ZDNet, https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last accessed June 13, 2025).

[17] Ransomware Guide, U.S. CISA, https://www.cisa.gov/stopransomware/ransomware-guide (last accessed June 13, 2025).

the Data Breach, Defendant, having elected to store the unencrypted Private Information of thousands of its current and former employees in an Internet-accessible environment, had reason to be on guard for the exfiltration of the Private Information and Defendant's type of business had cause to be particularly on guard against such an attack.

156. Before the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' Private Information could be accessed, exfiltrated, and published as the result of a cyberattack. Notably, data breaches are prevalent in today's society, therefore making the risk of experiencing a data breach entirely foreseeable to Defendant.

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

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

Defendant Failed to Follow FTC Guidelines

159. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. Thus, the FTC issued numerous guidelines identifying best data security practices that businesses—like Defendant—should use to protect against unlawful data exposure.

160. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[18] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

161. The guidelines also recommend that businesses watch for the transmission of large amounts of data out of the system—and then have a response plan ready for such a breach.

162. Furthermore, the FTC explains that companies must:

a. not maintain information longer than is needed to authorize a transaction;

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

163. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use 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

[18] *Protecting Personal Information: A Guide for Business,* FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

164. In short, Defendant's failure to use reasonable and appropriate measures to protect against unauthorized access to customers' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

165. Several best practices have been identified that—at a *minimum*—should be implemented by businesses like Defendant. These industry standards include: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption (making data unreadable without a key); multi-factor authentication; backup data; and limiting which employees can access sensitive data.

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

167. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04).

168. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Defendant opened the door to the criminals—thereby causing the Data Breach.

CLASS ACTION ALLEGATIONS

169. Plaintiffs bring this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3), as individuals and on behalf of all members of the following classes:

> All individuals residing in the United States whose PII was compromised in the Data Breach experienced by DISA in February 2024. (The "Nationwide Class").
>
> All individuals residing in California whose PII was compromised in the Data Breach experienced by DISA in February 2024 (the "California Subclass").

170. Excluded from the Classes are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant officer or director, any successor or assign, and any Judge who adjudicates this case, including their staff and immediate family.

171. Plaintiffs reserve the right to amend the class definition.

172. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on class-wide bases using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

173. Ascertainability. All members of the proposed Classes are readily ascertainable from information in Defendant's custody and control. After all, Defendant already identified some individuals and sent them data breach notices.

174. Numerosity. The Class members are so numerous that joinder of all Class members is impracticable. Upon information and belief, the proposed Class includes at least hundreds of thousands of members.

175. Typicality. Plaintiffs' claims are typical of Class members' claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

176. Adequacy. Plaintiffs will fairly and adequately protect the proposed Class's common interests. Their interests do not conflict with Class members' interests. And Plaintiffs have retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

177. Commonality and Predominance. Plaintiffs' and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class members—for which a class wide proceeding can answer for all Class members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's PII;

b. if 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. if Defendant were negligent in maintaining, protecting, and securing PII;

d. if Defendant breached contract promises to safeguard Plaintiffs and the Class's PII;

e. if Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Defendant's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiffs and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiffs and the Class are entitled to damages, treble damages, and or injunctive relief.

178. Superiority. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Class)

179. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 178 above as if fully set forth herein.

180. Plaintiffs and the Class, either directly or through their or their current and former employers, entrusted their PII to Defendant on the premise and with the understanding that

Defendant would safeguard their PII, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

181. Defendant owed a duty of care to Plaintiffs and Class members because it was foreseeable that Defendant's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII in a data breach. And here, that foreseeable danger came to pass.

182. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if their PII was wrongfully disclosed.

183. Defendant owed these duties to Plaintiffs and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiffs' and Class members' PII.

184. Defendant owed—to Plaintiffs and Class members—at least the following duties to:

a. exercise reasonable care in handling and using the PII in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiffs and Class members within a reasonable timeframe of any breach to the security of their PII.

185. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiffs and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required

and necessary for Plaintiffs and Class members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

186. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain under applicable regulations.

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

188. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class, either directly or their current and former employers, entrusted Defendant with their confidential PII, a necessary part of obtaining services from Defendant.

189. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII — whether by malware or otherwise.

190. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiffs' and Class members' and the importance of exercising reasonable care in handling it.

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

192. Defendant breached these duties as evidenced by the Data Breach.

193. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class members' PII by:

a. disclosing and providing access to this information to third parties and

b. failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

194. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiffs and Class members which actually and proximately caused the Data Breach and Plaintiffs' and Class members' injury.

195. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and Class members' injuries-in-fact.

196. Defendant has admitted that the PII of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

197. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

198. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and Class members actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

199. Plaintiffs re-allege and incorporate by reference paragraphs 1 through 178 above as if fully set forth herein.

200. Given the relationship between Defendant and Plaintiffs and Class members, where Defendant became guardian of Plaintiffs' and Class members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for Plaintiffs and Class members, (1) for the safeguarding of Plaintiffs' and Class members' PII; (2) to timely notify Plaintiffs and Class members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

201. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of Defendant's relationship with them—especially to secure their PII.

202. Because of the highly sensitive nature of the PII, Plaintiffs and Class members would not have entrusted Defendant, or anyone in Defendant's position, to retain their PII had they known the reality of Defendant's inadequate data security practices.

203. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to sufficiently encrypt or otherwise protect Plaintiffs and Class members' PII.

204. Defendant also breached its fiduciary duties to Plaintiffs and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

205. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

THIRD CAUSE OF ACTION
Violations of the California Consumer Privacy Act ("CCPA")
Cal. Civ. Code § 1798.150
(On behalf of Plaintiff Castro and the California Subclass)

206. Plaintiff Castro re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 178, as if fully set forth herein.

207. Defendant violated California Civil Code § 1798.150 of the CCPA by failing to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the nonencrypted Private Information of Plaintiff Castro and the California Subclass. As a direct and proximate result, Plaintiff's and the California Subclass's nonencrypted and nonredacted Private Information was subject to unauthorized access and exfiltration, theft, or disclosure.

208. Defendant is a "business" under the meaning of Civil Code § 1798.140 because Defendant is a "corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners" that "collects consumers' personal information" and is active "in the State of California" and "had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year." Civil Code §

1798.140(d).

209. Plaintiff Castro and Class Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards Private Information by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold Private Information, including Plaintiff Castro's and Class members' Private Information. Plaintiff Castro and Class members have an interest in ensuring that their Private Information is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

210. Pursuant to California Civil Code § 1798.150(b), Plaintiff Castro mailed a CCPA notice letter to Defendant's registered service agents, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. If Defendant cannot cure within 30 days—and Plaintiff believes such cure is not possible under these facts and circumstances—then Plaintiff intends to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

211. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information so as to protect the personal information under the CCPA.

212. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant.

FOURTH CAUSE OF ACTION
VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW
Cal. Bus. & Prof. Code § 17200, et seq. – Unlawful Business Practices]
(On Behalf of Plaintiff Castro and the California Subclass)

213. Plaintiff Castro re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 178, as if fully set forth herein.

214. Defendant violated Cal. Bus. and Prof. Code § 17200, et seq., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the California Subclass.

215. Defendant engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting the Private Information of Plaintiff Castro and Class Members with knowledge that the information would not be adequately protected; and by storing Plaintiff Castro's and Class Members' Private Information in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendant to take reasonable methods for safeguarding the Private Information of Plaintiff Castro and the Class Members.

216. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the Data Breach in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82.

217. As a direct and proximate result of Defendant's unlawful practices and acts, Plaintiff Castro and Class Members were injured and lost money or property, including but not limited to the price received by Defendant for the products and services, the loss of Plaintiff's and Class Members' legally protected interest in the confidentiality and privacy of their Personal Information, nominal damages, and additional losses as described herein.

218. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Plaintiff Castro's and Class Members' Private Information and that the risk of a data breach or theft was highly likely. Defendant's actions in engaging in the

above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of Plaintiff Castro and Class Members.

219. Plaintiff Castro, on behalf of the California Subclass, seeks relief under Cal. Bus. & Prof. Code § 17200, et seq., including, but not limited to, restitution to Plaintiff Castro and Class Members of money or property that Defendant may have acquired by means of its unlawful, and unfair business practices, disgorgement of all profits accruing to Defendant because of its unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

FIFTH CAUSE OF ACTION
VIOLATION OF THE CALIFORNIA CONSUMER RECORDS ACT
(On Behalf of Plaintiff Castro and the California Subclass)

220. Plaintiff Castro re-alleges and incorporates by reference all of the allegations contained in paragraphs 1 through 178, as if fully set forth herein.

221. Under the California Consumer Records Act, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believes to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82. The disclosure must "be made in the most expedient time possible and without unreasonable delay" but disclosure must occur "immediately following discovery [of the breach], if the personal information was, or is reasonable believes to have been, acquired by an unauthorized person." *Id.* (emphasis added).

222. The Data Breach constitutes a "breach of the security system" of Defendant.

223. An unauthorized person acquired the personal, unencrypted information of Plaintiff Castro and the California Subclass.

224. Defendant knew that an unauthorized person had acquired the personal, unencrypted information of Plaintiff Castro and the California Subclass but waited over a year to notify them. Given the severity of the Data Breach, this is an unreasonable delay.

225. Defendant's unreasonable delay prevented Plaintiff Castro and the California Subclass from taking appropriate measures from protecting themselves against harm.

226. Because Plaintiff Castro and the California Subclass were unable to protect themselves, they suffered incrementally increased damages that they would not have suffered with timelier notice.

227. Plaintiff Castro and the California Subclass are entitled to equitable relief and damages in an amount to be determined at trial.

PRAYER FOR RELIEF

Plaintiffs and Class members respectfully request judgment against Defendant and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiffs and the Class;

D. Awarding Plaintiffs and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

E. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

F. Awarding attorneys' fees and costs, as allowed by law;

G. Awarding prejudgment and post-judgment interest, as provided by law;

H. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

I. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial for all claims so triable.

Dated: June 30, 2025

Respectfully submitted,

/s/ Andrew J. Shamis
Andrew J. Shamis
SHAMIS GENTILE
14 NE 1 Ave., Suite 705
Miami, Florida 33132
Tel: (305) 479-2299
Fax: (786) 623-0915

J. Gerard Stanch, IV (admitted *Pro Hac Vice*)
STRANCH, JENNINGS & GARVEY, PLLC
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
Phone: (615) 254-8801
gstranch@stranchlaw.com

Jeff Ostrow (admitted *Pro Hac Vice*)
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd, Suite 500
Fort Lauderdale, FL 33301
Tel: (954) 525-4100
Fax: (954) 525-4300

ostrow@kolawyers.com

Attorneys for Plaintiffs and the Proposed Class

EXHIBIT A

Tuesday, February 25, 2025 at 09:08:20 Eastern Standard Time

[redacted]

- Ten4 TG

---------- Forwarded message ---------

[redacted]

February 24, 2025

Re: Notice of Data Incident

Dear CHRISTOPHER DUIKER,

DISA Global Solutions, Inc. ("DISA") is a third-party administrator of employment screening services, including drug and alcohol testing and background checks. We are writing to inform you about an incident experienced by DISA that may have involved some of your personal information, which came into our possession due to the employee screening services you may have completed with your current or former employer or a prospective employer. While we are unaware of any attempted or actual misuse of any information involved in this incident, we are providing you with information about the incident and steps you can take to protect yourself, should you feel it necessary.

What Happened?

On April 22, 2024, we discovered that we were the victim of a cyber incident that impacted a limited portion of our network. Upon discovery, we immediately contained the incident

and initiated an investigation with the assistance of third-party forensic experts. Our investigation determined that an unauthorized third party accessed our environment between February 9, 2024, and April 22, 2024, and procured some information. Although our forensics investigation could not definitively conclude the specific data procured, DISA conducted a detailed and time-intensive review of the affected files to identify the personal information contained therein. We are providing you this notice upon the recent completion of this review.

What Information Was Involved.

The affected files contained your name and the following: Social Security number, driver's license or state identification number. Presently, we have no evidence of actual or attempted misuse of your personal information.

What We Are Doing.

Upon discovery of the incident, we secured our environment, notified law enforcement authorities, safely restored our systems and operations, and implemented additional security measures. We are also notifying you so that you may take further steps to protect your information should you feel it appropriate to do so. In addition, we are providing you with access to 12 months of credit monitoring and identity restoration services through Experian at no charge to you. You must enroll by June 30, 2025.

What You Can Do.

Please review the enclosed "*Steps You Can Take to Help Protect Your Information*" which describes the services we are offering, how to activate them, and provides further details on how to protect yourself. We encourage you to remain vigilant against the potential for identity theft and fraud and to monitor your credit reports for any suspicious activity.

For More Information.

We sincerely regret any inconvenience this incident may have caused you. If you have additional questions, you may call our dedicated assistance line 833-931-9800 (toll-free), Monday–Friday, from 9:00 a.m. To 9:00 p.m. Eastern Time, or write to us at 11740 Katy Freeway, Suite 900, Houston, TX 77079.

Sincerely,

DISA Global Solutions, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Complimentary Identity Monitoring Services

We are providing you with a 12-month membership of Experian's IdentityWorks. A credit card is not required for enrollment in the identity monitoring services. To enroll, at no cost to you:

- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: [redacted]
- Ensure that you **enroll by**: June 30, 2025 (Your code will not work after this date.)

With Experian IdentityWorks, you can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers. The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

If you have questions about the product, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-931-9800 by June 30, 2025. Be prepared to provide engagement number B137497 as proof of eligibility for the identity restoration services by Experian.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 833-931-9800. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

Obtain a Free Credit Report

Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus (Equifax, Experian, and TransUnion). Obtaining a copy of your credit report from each agency on an annual basis, and reviewing it for suspicious activity, can help you spot problems and address them quickly. You can request your free credit report online at www.annualcreditreport.com or by phone at 1-877-322-8228. You can also request your free credit report by completing the request form at: www.annualcreditreport.com, and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

Place a Fraud Alert

As a precaution against identity theft, you can consider placing a fraud alert on your credit file. A "fraud alert" tells creditors to contact you before opening a new account or changing an existing account. A fraud alert also lets your creditors know to watch for unusual or suspicious activity. To place a fraud alert, call any one of the three major credit reporting agencies listed below. An initial fraud alert remains effective for ninety days, and is free of charge. If you wish, you can renew the fraud alert at the expiration of this initial period. As soon as one credit agency confirms your fraud alert, the others are notified to place fraud alerts on your file.

Equifax®
P.O. Box 105069
Atlanta, GA 30348-5069
1-800-685-1111
www.equifax.com/personal/credit-report-services/

Experian
P.O. Box 9554
Allen, TX 75013-9701
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion®
P.O. Box 2000
Chester, PA 19016-1000
1-800-680-7289
https://www.transunion.com/fraud-alerts

Place a Security Freeze

Federal law also allows consumers to place, lift or remove a security freeze on their credit reports at no charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. Be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services.

To place a security freeze on your credit report, you must send a written request by regular, certified, or overnight mail at the addresses below to each of the three major credit reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com). You may also request the security freeze through each of the credit reporting agencies' websites or over the phone:

Equifax®
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045
www.equifax.com/personal/help/place-lift-remove-security-freeze/

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion®
.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
https://www.transunion.com/credit-freeze

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

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft; and
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

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

To lift the security freeze in order to allow a specific entity or individual access to your

credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Additional Information

You may obtain additional information about identity theft (including, a security freeze) by contacting the above, the Federal Trade Commission (FTC), or your state Attorney General, or the Federal Trade Commission (FTC). The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. You are advised to report known or suspected identity theft to law enforcement, including your state's Attorney General and the FTC. Under the law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft or fraud, you also have the right to file a police report and obtain a copy of it. Notice was not delayed as a result of law enforcement.

For District of Columbia residents, the Attorney General can be contacted at 400 6th Street NW, Washington, D.C. 20001, oag.dc.gov, or 202-727-3400.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, oag.state.md.us, or 888-743-0023. We can be contacted at 10900 Corporate Centre Dr Ste 250, Houston, Texas, 77041.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information and the consumer reporting agencies may not report outdated negative information. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have

specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

For New York residents, the Attorney General can be contacted at The Capitol, Albany, NY, 12224, ag.ny.gov, or 800-771-7755.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699, ncdoj.gov, or 919-716-6000.

For Rhode Island residents, the Attorney General can be contacted at 150 South Main Street, Providence, RI, 02903, www.riag.ri.gov, or 401-274-4400.