UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
BALTIMORE DIVISION

CHEALESA PARSHA and LYDIA JARRELL, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

ZEROED-IN TECHNOLOGIES, LLC

Serve: Registered Agent
Keith A. Good
780 Elkridge Landing Road
Linthicum, MD 21090

and

DOLLAR TREE, INC.

Serve: Corporation Service Company
Shockoe Slip, Floor 2
Richmond, VA 23219

and

FAMILY DOLLAR, LLC

Serve: Corporation Service Company
2626 Glenwood Avenue
Suite 550
Richmond, VA 27608

Defendants.

CASE NO.:

CLASS ACTION COMPLAINT

(1) Negligence;
(2) Breach of Implied Contract;
(3) Unjust Enrichment/Quasi-Contract;
(4) Breach of Confidence
(5) Injunctive/Declaratory Relief

DEMAND FOR JURY TRIAL

Plaintiffs Chealesa Parsha and Lydia Jarrell ("Plaintiffs"), individually and on behalf of all others similarly situated ("Class members"), allege against Zeroed-In Technologies, LLC ("Zeroed-In"), Dollar Tree, Inc. ("Dollar Tree"), and Family Dollar, LLC ("Family Dollar") (collectively, the "Defendants"), upon personal knowledge as to their own actions and their

counsel's investigations, and upon information and belief as to all other matters, the following:

1. Plaintiffs bring this Class Action Complaint against Defendants for their failure to exercise reasonable care in securing and safeguarding Plaintiffs' and Class members' sensitive personal data, including, but not limited to, names, dates of birth, and Social Security numbers (collectively, "Private Information").

2. Defendant Dollar Tree is a publicly traded company, trading under the symbol DLTR on the Nasdaq stock exchange with revenue of $28.332 billion in 2023.[1]

3. As the result of a 2015 merger, Dollar Tree's corporate personnel includes employees at both Dollar Tree and Family Dollar store locations.[2]

4. Defendant Zeroed-In offers workforce analytics and data management software to more than 70 clients— including Dollar Tree and Family Dollar— and has more than 30,000 registered users.[3]

5. In August of 2023, Zeroed-In discovered unusual activity on its computer systems. Specifically, Zeroed-In asserts that an unauthorized third party accessed its networks containing Private Information, including that of Dollar Tree and Family Dollar store employees, between August 7, 2023 and August 8, 2023 (the "Data Breach"). As a result, the Private Information of thousands of individuals was compromised.

6. Plaintiffs did not receive breach notification letters until December of 2023. Defendants' failure to timely notify Plaintiffs and Class members about the Data Breach for four (4) months left them particularly vulnerable.

---

[1] https://corporate.dollartree.com/investors/financial-information/financial-results (Last visited Dec. 7, 2023)

[2] *Dollar Tree Completes Acquisition of Family Dollar*, Dollar Tree Inc. (July 6, 2015), https://corporate.dollartree.com/news-media/press-releases/detail/120/dollar-tree-completes-acquisition-of-family-doll

[3] https://www.zeroedin.com/how-it-works/ (Last visited Dec. 7, 2023)

7. Defendants' security failures enabled the hackers to steal the Private Information of Plaintiffs and members of the Class (defined below). These failures put Plaintiffs' and Class members' Private Information and interests at serious, immediate, and ongoing risk and, additionally, caused costs and expenses to Plaintiffs and Class members associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including, as appropriate, reviewing records for fraudulent charges, cancelling and reissuing payment cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, initiating and monitoring credit freezes, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach.

8. The Data Breach was caused and enabled by Defendants' violation of their obligations to abide by best practices, industry standards, and federal and state laws concerning the security of individuals' Private Information. Defendants knew or should have known that their failure to take reasonable security measures— which could have prevented or mitigated the Data Breach that occurred— left Plaintiffs' and Class members' Private Information vulnerable to identity theft, financial loss, and other associated harms.

9. Accordingly, Plaintiffs assert claims for negligence, breach of implied contract, unjust enrichment/quasi-contract, and breach of confidence.

10. Plaintiffs also seek injunctive relief, monetary damages, statutory damages, and all other relief as authorized in equity or by law.

PARTIES

A. PLAINTIFF CHEALESA PARSHA

11. Plaintiff Chealesa Parsha is a resident and citizen of Arkansas, and brings this action in her individual capacity and on behalf of all others similarly situated.

12. Plaintiff is a former employee of a Dollar Tree located in Magnolia, Arkansas, where she worked from approximately May 2020 to April 2023.

13. In the regular course of business for hiring and employment purposes, Dollar Tree collected, stored, and utilized Plaintiff's Private Information and shared it with Zeroed-In, which maintained, stored, and utilized that Information.

14. In storing Plaintiff's Private Information, Defendants expressly and impliedly promised to safeguard it. Defendants, however, did not implement proper, industry-standard safeguards to protect Plaintiff's Private Information, leading to its exposure and exfiltration by cybercriminals, who stole the Private Information at issue with the intent to sell it and/or fraudulently misuse it for their own gain.

15. On December 4, 2023, Plaintiff received a notification letter from Zeroed-In stating that her Private Information was compromised by cybercriminals.

16. Since the occurrence of the Data Breach in August 2023, Plaintiff attempted to apply for a loan with Western Finance. She was told by a loan officer that her application was rejected due to fraud associated with her Social Security Number.

17. Plaintiff and Class members have faced and will continue to face a certainly impending and substantial risk of future harms because of Defendants' ineffective data security measures, as further set forth herein.

18. Plaintiff Parsha greatly values her privacy and would not have chosen to disclose her Private Information to Defendants if she had known they would negligently maintain it as they did.

B. PLAINTIFF LYDIA JARRELL

19. Plaintiff Lydia Jarrell is a resident and citizen of Oregon, and brings this action in her individual capacity and on behalf of all others similarly situated.

20. Plaintiff is a former employee of Dollar Tree, having worked at a Family Dollar store location in Pendleton, Oregon for approximately one month in November 2021.

21. In the regular course of business for hiring and employment purposes, Dollar Tree obtained, collected, stored, and utilized Plaintiff's Private Information and shared it with Zeroed-

In, which maintained, stored, and utilized that Information.

22. In storing Plaintiff's Private Information, Defendants expressly and impliedly promised to safeguard it. Defendants, however, did not implement proper, industry-standard safeguards to protect Plaintiff's Private Information, leading to its exposure and exfiltration by cybercriminals, who stole the Private Information at issue with the intent to sell it and/or fraudulently misuse it for their own gain.

23. On December 6, 2023, Plaintiff received a notification letter from Zeroed-In stating that her Private Information was compromised by cybercriminals.

24. Since the occurrence of the Data Breach in August 2023, Plaintiff experienced fraudulent charges on one of her credit cards in Hershey, Pennsylvania, where she has never been. In addition, someone used her name to open a new credit card account in Washington state.

25. Plaintiff and Class members have faced and will continue to face a certainly impending and substantial risk of future harms because of Defendants' ineffective data security measures, as further set forth herein.

26. Plaintiff Jarrell greatly values her privacy and would not have chosen to disclose her Private Information to Defendants if she had known they would negligently maintain it as they did.

C. DEFENDANT ZEROED-IN TECHNOLOGIES

27. Defendant Zeroed-In Technologies, LLC is a Florida registered limited liability corporation with its principal place of business located at 780 Elkridge Landing Road, Suite 208, Linthicum, Maryland.

28. Zeroed-In is a data technology company that sells workforce analytical software to its clients. The software uses artificial intelligence to "monetize HR's data science activities" so that its clients can "make accurate and timely HR decisions."[4]

[4] https://www.zeroedin.com/how-it-works/ (Last visited Dec. 7, 2023)

29. Upon information and belief, members of Zeroed-In Technologies include Keith A. Goode and Chris Moore. Upon investigation of counsel, Keith Goode is domiciled in the state of Maryland, where public records indicate he resides and intends to stay.[5]

D. DEFENDANT DOLLAR TREE

30. Defendant Dollar Tree, Inc. is a publicly traded corporation incorporated in Virginia with its principal place of business located at 500 Volvo Parkway, Chesapeake, Virginia 23320.

31. Defendant Dollar Tree acquired Defendant Family Dollar in 2015 and the companies merged.[6]

32. As the result of the merger, Dollar Tree owns and operates more than 16,600 retail discount store locations across the United States and Canada under two names, Dollar Tree and Family Dollar.

E. DEFENDANT FAMILY DOLLAR

33. Defendant Family Dollar, LLC was formed in North Carolina and has its principal place of business located at 500 Volvo Parkway, Chesapeake, Virginia 23320.

JURISDICTION AND VENUE

34. The Court has subject matter and diversity jurisdiction over Plaintiffs' claims under 28 U.S.C. § 1332(d)(2) ("CAFA") because a) this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, b) there are

---

[5] https://www.linkedin.com/in/keith-goode-9a83571/ (Last visited Dec. 7, 2023).

[6] *Dollar Tree Completes Acquisition of Family Dollar*, Dollar Tree Inc. (July 6, 2015), https://corporate.dollartree.com/news-media/press-releases/detail/120/dollar-tree-completes-acquisition-of-family-dollar

more than 100 members in the proposed class, and c) at least one member of the Class is a citizen of a different state than Defendants (including both Plaintiffs), which establishes minimal diversity.

33. The Court has general personal jurisdiction over Defendant Zeroed-In because one or more of its members resides in Maryland and this District; because it operates and conducts substantial business in Maryland and this District, and because the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from Maryland and this District.

34. The Court has general personal jurisdiction over Defendants Dollar Tree and Family Dollar because they shared Plaintiffs' and Class members' Private Information with Defendant Zeroed-In, in Maryland and this District.

35. Venue is proper in this District under 28 U.S.C. §1391(b) because Zeroed-In operates in this District; Dollar Tree and Family Dollar provided and entrusted Plaintiffs' and Class members' Private Information to Zeroed-In in this District; a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District; and Defendants have harmed Class members residing in this District.

FACTUAL ALLEGATIONS

36. Plaintiffs and Class Members are current and former employees at Zeroed-In's clients, including Dollar Tree and Family Dollar.

37. Zeroed-In requires its clients' employees, including Plaintiff and Class Members, to submit non-public Private Information in the ordinary course of providing its services.

37. As a condition of obtaining employment at Zeroed-In's clients, Plaintiffs and Class Members were thus required to entrust all Defendants, directly or indirectly, with highly sensitive Private Information.

38. The information held by Defendants in their computer systems or those of their vendors at the time of the Data Breach included the unencrypted Private Information of Plaintiffs and Class Members.

39. Upon information and belief, Defendants made promises and representations to its clients' employees, including Plaintiffs and Class Members, that the Private Information collected from them as a condition of obtaining employment at Zeroed-In's clients would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendants would delete any sensitive information after they were no longer required to maintain it.

40. Indeed, Zeroed-In's Privacy Policy provides that: "[w]e employ robust security measures to protect against the loss, misuse and alternation of the personal information under our control. The Sites employ Secure Socket Layer (SSL) technology using both server authentication and data encryption. The Sites are hosted in a secure server environment that uses firewalls, intrusion detection systems, and other advanced technology to protect against interference or access from outside intruders."[7]

41. Similarly, Dollar Tree's Privacy Policy provides that: "[w]e use various reasonable and appropriate safeguards (administrative, organizational, technical, electronic, procedural, and physical) to protect the Personal Information we collect and process. Our security controls are designed to maintain an appropriate level of confidentiality, integrity, and availability of your Personal Information."[8]

42. Family Dollar's Privacy Policy provides that: "[w]e use various reasonable and appropriate safeguards (administrative, organizational, technical, electronic, procedural, and

---

[7] https://www.zeroedin.com/privacy-policy/ (Last visited December 7, 2023).

[8] https://www.dollartree.com/privacy-policy (Last visited December 7, 2023).

physical) to protect the Personal Information we collect and process. Our security controls are designed to maintain an appropriate level of confidentiality, integrity, and availability of your Personal Information."[9]

43. Plaintiffs and Class Members provided their Private Information, directly or indirectly, to Defendants with the reasonable expectation and on the mutual understanding that Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access.

44. On or around November 27, 2023, Zeroed-In issued Notice Letters to its clients' Employees, including Plaintiffs and Class members, alerting them that their sensitive Private Information had been exposed in a Data Breach. The Notice Letter offered 12 months of free credit monitoring and included generic information about identity protection including steps that victims of data security incidents can take, such as examining account statements, getting a copy of a free annual credit report or implementing a fraud alert or security freeze.

45. Based on the Notice Letter sent to Plaintiffs and Class members, Defendants were alerted to unusual activity indicating unauthorized access to its computer systems in August of 2023. This means that Plaintiffs and Class members had no knowledge their Private Information was comprised for nearly four (4) months after Defendants first learned of the Data Breach.

46. Defendants offered no explanation for the delay between the initial discovery of the Breach and the belated notification to affected individuals– delay that resulted in Plaintiff and Class members suffering harm they otherwise could have avoided had a timely disclosure been made.

---

[9] https://www.familydollar.com/privacy-policy (Last visited Dec. 7, 2023).

47. Further, the offer contained in the Notice Letter to provide 12 months of credit monitoring is woefully inadequate. Credit monitoring only alerts individuals to the misuse of their information after it happens, which might not take place until years after the Data Breach.

48. The Data Breach occurred because Defendants failed to take reasonable measures to protect the Private Information they collected and stored. Among other things, Defendants failed to implement data security measures designed to prevent this attack, despite repeated warnings about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past on other HR software providers.

49. Defendants disregarded the rights of Plaintiffs and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs and Class members' Private Information was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data. As a result, the Private Information of Plaintiffs and Class members was exfiltrated through unauthorized access by an unknown, malicious cyber hacker with the intent to fraudulently misuse it. Plaintiffs and Class members have a continuing interest in ensuring that their compromised Information is and remains safe.

A. Defendants Failed to Comply with Industry Standards and Federal and State Law

50. As a condition of obtaining employment at Zeroed-In's clients, Dollar Tree and Family Dollar, Plaintiffs and Class Members were required to entrust all three Defendants, directly or indirectly, with highly sensitive Private Information.

51. By obtaining, collecting, using, and deriving a benefit from Plaintiffs and Class members' Private Information, Defendants assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs and Class members' Private Information from disclosure.

52. Defendants had obligations created by industry standards and federal and state law to keep Class members' Private Information confidential and to protect it from unauthorized access and disclosure.

53. Plaintiffs and Class members provided their Private Information to Defendants with the reasonable expectation and mutual understanding that Defendants would comply with its obligation to keep such information confidential and secure from unauthorized access.

54. Defendants' failure to provide adequate security measures to safeguard Plaintiffs' and Class members' Private Information is especially egregious because Defendants operate in a field which has recently been a frequent target of scammers attempting to fraudulently gain access to customers' Private Information. Cyber security professionals have consistently identified human resources platforms as particularly vulnerable to data breaches because of the value of the Private Information they collect and maintain.

55. The number of US data breaches surpassed 1,800 in 2021, a record high and a sixty-eight percent increase in the number of data breaches from the previous year.[10]

56. In August 2022, the Consumer Finance Protection Bureau (CFPB) published a circular on data security. The CFPB noted that "[w]idespread data breaches and cyberattacks have resulted in significant harms to [individuals], including monetary loss, identity theft, significant time and money spent dealing with the impacts of the breach, and other forms of financial distress," and the circular concluded that the provision of insufficient security for individuals' data can violate the prohibition on "unfair acts or practices" in the Consumer Finance Protection Act (CFPA).[11]

57. Charged with handling sensitive Private Information, Defendants knew, or should

---

[10] Identity Theft Resource Center, *2021 Annual Data Breach Year-End Review*, https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/

[11] CONSUMER FIN. PROT. BUREAU, *Consumer Financial Protection Circular 2022-04: Insufficient data protection or security for sensitive consumer information* (Aug. 11, 2022), https://files.consumerfinance.gov/f/documents/cfpb_2022-04_circular_2022-08.pdf.

have known, the importance of safeguarding individuals' Private Information that was entrusted to them and of the foreseeable consequences if their data security systems were breached. This includes the significant costs that would be imposed on Plaintiffs and Class members after a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

58. Despite the abundance and availability of information regarding cybersecurity best practices for HR management platforms, Defendants chose to ignore them. These best practices were known, or should have been known by Defendants, whose failure to heed and properly implement them directly led to the Data Breach and the unlawful exposure of Private Information.

59. At a minimum, industry best practices should have been implemented by Defendants, including but not limited to requiring users to create strong passwords; implementing multi-layer security including firewalls and anti-malware software; encrypting data and making it unreadable without a key; updating and patching all systems with the latest security software; and better educating its employees about safe data security practices.

60. Defendants apparently did not follow these precautions because cybercriminals accessed individuals' Private Information off Zeroed-In's network until Zeroed-In was able to cease the unauthorized access.

61. Defendants were also on notice that under the FTC Act, Defendants are prohibited from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for individuals' sensitive personal information is an "unfair practice" in violation of the FTC Act.[12]

62. Defendants are further required by the comprehensive data privacy regimes enacted by at least 13 states to protect Plaintiffs' and Class members' Private Information, and further, to handle any breach of the same in accordance with applicable breach notification

---

[12] *See, e.g., FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

statutes.[13]

63. The potential for improper disclosure of Plaintiffs' and Class members' Private Information was a known risk to Defendants, and thus Defendants were was on notice that failing to take reasonable steps necessary to secure the Private Information from those risks left the Private Information in a vulnerable position.

B. Defendants Exposed the Class to Identity Theft, Financial Loss, and Other Harms

64. Plaintiffs and Class members have been injured by the disclosure of their Private Information in the Data Breach.

65. The fact that Plaintiffs' and Class members' Private Information was stolen means that Class members' information is likely for sale by cybercriminals and will be misused in additional instances in the future.

66. Private Information is a valuable commodity to identity thieves. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identify theft and financial fraud.[14] Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground Internet websites, commonly referred to as the dark web.

67. The value of Plaintiffs' and Class members' Private Information on the black market is substantial. Indeed, studies confirm that the average direct financial loss for victims of identity theft in 2014 was $1,349.[15]

68. The FTC has also recognized that personal data is a valuable form of currency. In

---

[13] International Association of Privacy Professionals, *Delaware Governor Signs Personal Data Privacy Act* (Sep. 12, 2023), https://iapp.org/news/a/delaware-governor-signs-personal-data-privacy-act.

[14] Federal Trade Commission, *Warning Signs of Identity Theft* (Sept. 2018), https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft .

[15] *See* U.S. Dep't of Justice, *Victims of Identity Theft*, OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

an FTC roundtable presentation, a former Commissioner, Pamela Jones Harbour, underscored this point:

> Most [people] cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis—and profit.[16]

69. Recognizing the high value that individuals place on their Private Information, many companies now offer individuals an opportunity to sell this information.[17] The idea is to give individuals more power and control over the type of information that they share and who ultimately receives that information. And, by making the transaction transparent, individuals will make a profit from their Private Information. This business has created a new market for the sale and purchase of this valuable data.

70. At all relevant times, Defendants were well-aware, or reasonably should have been aware, that the Private Information they maintain is highly sensitive and could be used for wrongful purposes by third parties, such as identity theft and fraud.

71. Had Defendants remedied the deficiencies in their security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, Defendant would have prevented the breach of its systems and, ultimately, the theft of Plaintiffs' and Class members' Private Information.

72. The compromised Private Information in the Data Breach is of great value to hackers and thieves and can be used in a variety of ways. Information about an individual that can be logically associated with other information can be chained together, increasing its utility

---

[16] *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMM'N (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

[17] *Web's Hot New Commodity*, *supra* note 17.

to criminals.

73. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the "mosaic effect."

74. In short, the Private Information exposed is of great value to hackers and cyber criminals and the data compromised in the Data Breach can be used in a variety of unlawful manners, including opening new credit and financial accounts in users' names.

C. Plaintiffs and Class Members Suffered Damages from the Data Breach

75. Plaintiffs and the Class have been damaged by the compromise of their Private Information in the Data Breach.

76. The ramifications of Defendants' failure to keep the Class's Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to the victims may continue for years. Victims of data breaches are more likely to become victims of identity fraud.[18]

77. In addition to its obligations under state and federal laws and regulations, Defendants owed a common law duty to Plaintiffs and Class members to protect the Private Information they entrusted to it, including to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized parties.

78. Defendant further owed and breached its duty to Plaintiffs and Class members to implement processes and specifications that would detect a breach of its security systems in a timely manner and to timely act upon warnings and alerts, including those generated by its own security systems.

79. As a direct result of Defendants' intentional, willful, reckless, and negligent

[18] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf.

conduct which resulted in the Data Breach, unauthorized parties were able to access, acquire, view, publicize, and/or otherwise commit the identity theft and misuse of Plaintiffs' and Class members' Private Information as detailed above, and Plaintiffs and members of the Class are at a heightened and increased substantial risk of suffering identity theft and fraud.

80. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some individuals victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

81. Some of the injuries and risks associated with the loss of personal information have already manifested themselves in Plaintiffs and other Class members' lives. Plaintiff incurred unauthorized charges on her credit card on August 14.

82. Plaintiffs and the Class continue to face a substantial risk of suffering out-of-pocket fraud losses such as fraudulent charges on online accounts, credit card fraud, applications for benefits made fraudulently in their names, loans opened in their names, medical services billed in their names, government benefits fraudulently drawn in their name, and identity theft. Many Class members may already be victims of identity theft and fraud without realizing it.

83. Plaintiffs and Class members have, may have, and/or will have incurred out of pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

84. Plaintiffs and Class members did not receive the full benefit of their bargain when exchanging their private personal data for Defendants' services as an employer. In exchange, Plaintiffs and Class Members should have received from Dollar Tree the employment positions that were the subject of the transaction and should also have been entitled to have Defendants protect their Private Information with adequate data security.

85. Plaintiffs and Class members were damaged in an amount at least equal to the difference in the value between the services they thought they (which would have included

adequate data security protection) and the services they actually received.

86. Plaintiffs and Class members would not have obtained services from Defendant had they known that Defendant failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data security practices to safeguard their Private Information from criminal theft and misuse.

87. Plaintiffs and the Class will continue to spend significant amounts of time to monitor their financial accounts for misuse.

88. Identity thieves can use the victim's Private Information to commit any number of frauds, such as obtaining a job, procuring housing, or even giving false information to police during an arrest. As a result, Plaintiffs and Class members now face a real and continuing immediate risk of identity theft and other problems associated with the disclosure of their Social Security numbers and will need to monitor their credit for an indefinite duration. Defendants knew or should have known this and strengthened their data systems accordingly. Defendants were put on notice of the substantial and foreseeable risk of harm from a data breach, yet they failed to properly prepare for that risk.

89. As a result of the Data Breach, Plaintiffs and Class members' Private Information has diminished in value.

90. The Private Information belonging to Plaintiffs and Class members is private and was left inadequately protected by Defendant who did not obtain Plaintiffs' or Class members' consent to disclose such Private Information to any other person as required by applicable law and industry standards. Defendants disclosed Plaintiffs' and Class members' Private Information as a direct result of its inadequate security measures.

91. The Data Breach was a direct and proximate result of Defendant's failure to: (a) properly safeguard and protect Plaintiff and Class members' Private Information from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff and Class members' Private Information; and (c) protect against reasonably foreseeable threats to the

security or integrity of such information.

92. Defendants had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligation to protect customer data.

93. Defendants did not properly train their employees, particularly its information technology department, to timely identify cyber attacks and other data security risks.

94. Had Defendants remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented the intrusions into its systems and, ultimately, the theft of Plaintiffs and Class members' Private Information.

95. As a direct and proximate result of Defendants' wrongful actions and inactions, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

96. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[19]

97. Other than offering 12 months of credit monitoring, Defendants did not take any measures to assist Plaintiffs and Class members.

98. The limited offer of credit monitoring is woefully inadequate. While some harm has already taken place, the worst is yet to come. There may be a time lag between when harm occurs versus when it is discovered, and between when Private Information is acquired and when it is used. Furthermore, identity theft monitoring only alerts someone to the fact that they have

---

[19] *See* U.S. Dep't of Justice, *Victims of Identity Theft*, OFFICE OF JUSTICE PROGRAMS: BUREAU OF JUSTICE STATISTICS 1 (Nov. 13, 2017), https://www.bjs.gov/content/pub/pdf/vit14.pdf [hereinafter *Victims of Identity Theft*].

already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's Private Information) – it does not prevent identity theft.[20]

99. Defendants' failure to adequately protect Plaintiffs' and Class members' Private Information has resulted in Plaintiffs and Class members having to undertake these tasks, which require extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of money–while Defendants sit by and does nothing to assist those affected by the incident. Instead, as Zeroed-In's notice confirms, the burden is on Plaintiffs and Class members to discover possible fraudulent activity and identity theft and mitigate the negative impacts arising from such fraudulent activity on their own.

100. Plaintiffs and Class members have been damaged in several other ways as well. Plaintiffs and Class members have been exposed to an impending, imminent, and ongoing increased risk of fraud, identity theft, and other misuse of their Private Information. Plaintiffs and Class members must now and indefinitely closely monitor their financial and other accounts to guard against fraud. This is a burdensome and time-consuming task. Class members have also been forced to purchase adequate credit reports, credit monitoring and other identity protection services, and have placed credit freezes and fraud alerts on their credit reports, while also spending significant time investigating and disputing fraudulent or suspicious activity on their accounts. Plaintiffs and Class members also suffered a loss of the inherent value of their Private Information.

101. The Private Information stolen in the Data Breach can be misused on its own or can be combined with personal information from other sources such as publicly available information, social media, etc. to create a package of information capable of being used to commit further identity theft. Thieves can also use the stolen Private Information to send spear-phishing emails to Class members to trick them into revealing sensitive information. Lulled by a

---

[20] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-beworth-the-cost.html.

false sense of trust and familiarity from a seemingly valid sender (for example Wells Fargo, Amazon, or a government entity), the individual agrees to provide sensitive information requested in the email, such as login credentials, account numbers, and the like.

102. As a result of Defendants' failures to prevent the Data Breach, Plaintiffs and Class members have suffered, will suffer, and are at increased risk of suffering:

- The compromise, publication, theft and/or unauthorized use of their Private Information;
- Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;
- Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from 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 and fraud;
- The continued risk to their Private Information, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake appropriate measures to protect the Private Information in their possession;
- Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and Class members; and
- Anxiety and distress resulting fear of misuse of their Private Information.

103. In addition to a remedy for the economic harm, Plaintiffs and Class members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

116. Plaintiffs bring all counts, as set forth below, individually and as a class action, pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure, on behalf of a "Nationwide Class" (collectively, the "Class") defined as:

Nationwide Class

> All persons who submitted their Private Information to Defendants and whose Private Information was compromised as a result of the data breach(es) discovered in or about August 2023.

117. Excluded from the Class are Defendants and Defendants' affiliates, parents, subsidiaries, employees, officers, agents, and directors. Also excluded is any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

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

119. **Numerosity**—Federal Rule of Civil Procedure 23(a)(1). The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, the Class has thousands of members.

120. **Commonality and Predominance**—Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3). Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, inter alia:

a. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, e.g., FTCA (as discussed below);

b. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

c. Whether Defendants properly implemented their purported security measures to protect Plaintiff's and the Class's Private Information from unauthorized capture, dissemination, and misuse;

d. Whether Defendants took reasonable measures to determine the extent of the Data Breach after they first learned of same;

e. Whether Defendants disclosed Plaintiffs' and the Class's Private Information in violation of the understanding that the Private Information was being disclosed in confidence and should be maintained;

f. Whether Defendants' conduct constitutes breach of an implied contract;

g. Whether Defendants willfully, recklessly, or negligently failed to maintain and execute reasonable procedures designed to prevent unauthorized access to Plaintiffs' and the Class's Private Information;

h. Whether Defendants were negligent in failing to properly secure and protect Plaintiffs' and the Class's Private Information;

i. Whether Defendants were unjustly enriched by their actions; and

j. Whether Plaintiffs and the Class are entitled to damages, injunctive relief, or other equitable relief, and the measure of such damages and relief.

121. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and other members of the Class. Similar or identical common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

122. **Typicality**—Federal Rule of Civil Procedure 23(a)(3). Plaintiffs' claims are typical of the claims of the other members of the Class because, among other things, all Class members were similarly injured through Defendants' uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendants that are unique to these Plaintiffs.

123. **Adequacy of Representation**—Federal Rule of Civil Procedure 23(a)(4). Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class they seeks to represent, they have retained counsel competent and experienced in complex class action litigation, and Plaintiffs will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiffs and their counsel.

124. **Injunctive Relief**—Federal Rule of Civil Procedure 23(b)(2). Defendants have acted and/or refused to act on grounds that apply generally to the Class, making injunctive and/or declaratory relief appropriate with respect to the Class under Fed. Civ. P. 23 (b)(2).

125. **Superiority**—Federal Rule of Civil Procedure 23(b)(3). A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for members of the Class to individually seek redress for Defendants' wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of the Nationwide Class)

126. Plaintiffs fully incorporate by reference all the above paragraphs, as though fully set forth herein.

127. Upon Defendants' accepting and storing the Private Information of Plaintiffs and the Class in their computer systems and on their networks, Defendants undertook and owed a duty to Plaintiffs and the Class to exercise reasonable care to secure and safeguard that information and to use commercially reasonable methods to do so. Defendants knew that Class members' Private Information was private and confidential and should be protected as private and confidential.

128. Defendants owed a duty of care not to subject Plaintiffs' and Class members' Private Information to an unreasonable risk of exposure and theft because Plaintiffs and Class members were foreseeable and probable victims of any inadequate security practices.

129. Defendants owed numerous duties to Plaintiff and the Class, including the following:

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

b. to protect Private Information using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

130. Defendants also breached their duty to Plaintiffs and Class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering their dilatory practices, Defendants failed to provide adequate supervision and oversight of the Private Information with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiffs' and Class members' Private Information and potentially misuse it and intentionally disclose it to others without consent.

131. Defendants knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendants knew or should have known about numerous well-publicized data breaches within the HR software industry.

132. Defendants knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiffs' and Class members' Private Information.

133. Defendants were in the position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

134. Defendants breached their duties to Plaintiffs and Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Private Information.

135. Because Defendants knew that a breach of their systems would damage thousands of individuals, including Plaintiffs and Class members, Defendants had a duty to adequately protect their data systems and the Private Information contained thereon.

136. Defendants' duty of care to use reasonable security measures arose from of the special relationship that existed between Defendants and users of its human resources software, which is recognized by data privacy laws and regulations under the laws of 13 states.

137. In addition, Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 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.

138. Defendants' 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 Defendants are bound by industry standards to protect confidential Private Information.

139. Defendants' own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their Private Information. Defendants' misconduct included failing to: (1) secure Plaintiffs' and Class members' Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

140. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class members' Private Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information;

b. Failing to adequately monitor the security of Defendant's networks and systems;

c. Allowing unauthorized access to Class members' Private Information;

d. Failing to detect in a timely manner that Class members' Private Information had been compromised; and

e. Failing to timely notify Class members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

141. Through Defendants' acts and omissions described in this Complaint, including their failure to provide adequate security and its failure to protect Plaintiffs' and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiffs' and Class members' Private Information during the time it was within Defendants' possession or control.

142. Defendants' conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to failing to adequately protect the Private Information and failing to provide Plaintiffs and Class members with timely notice that their sensitive Private Information had been compromised.

143. Neither Plaintiffs nor the other Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

144. As a direct and proximate cause of Defendants' conduct, Plaintiffs and Class members suffered damages as alleged above.

145. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all Class members.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of the Nationwide Class)

146. Plaintiffs fully incorporate by reference all the above paragraphs, as though fully set forth herein.

147. As a condition of their employment, Plaintiffs and Class members were required to provide Defendants with their Private Information.

148. In so doing, Plaintiff and Class members entered into implied contracts with all Defendants pursuant to which Defendants agreed to safeguard and protect such information and to timely detect any breaches of their Private Information. In entering into such implied contracts, Plaintiffs and Class members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

149. Plaintiffs and Class members would not have provided and entrusted their Private Information to Defendants in the absence of the implied contract between them and Defendants.

150. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendants.

151. Defendants breached the implied contracts they made with Plaintiffs and Class members by failing to safeguard and protect their Private Information and by failing to detect the Data Breach within a reasonable time.

152. As a direct and proximate result of Defendants' breaches of the implied contracts between Defendants, Plaintiffs, and Class members, Plaintiffs and Class members sustained actual losses and damages as described in detail above.

153. Plaintiffs and Class members are also entitled to injunctive relief requiring

Defendants 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 free credit monitoring to all Class members.

COUNT III
UNJUST ENRICHMENT/QUASI-CONTRACT
(On Behalf of the Nationwide Class)

154. Plaintiffs fully incorporate by reference all the above paragraphs, as though fully set forth herein.

155. Plaintiffs and Class members conferred monetary benefits on Defendants when they exchanged their sensitive Private Information for employment positions.

156. In exchange, Plaintiffs and Class Members should have received the employment positions that were the subject of the transactions. Plaintiffs and the Class were entitled to assume their employment included adequate data security for their Private Information.

157. Defendants knew that Plaintiffs and Class members conferred benefits upon them and have accepted and retained that benefit by accepting and retaining the Private Information entrusted to them. Defendants profited from Plaintiffs' and Class members' retained data and used Plaintiffs' and Class members' Private Information for business purposes.

158. Defendant failed to secure Plaintiffs' and Class members' Private Information and, therefore, did not provide full compensation for the benefit the Plaintiffs' and Class members' payments and Private Information provided.

159. Defendants acquired the Private Information through inequitable means as they failed to disclose the inadequate security practices previously alleged.

160. If Plaintiffs and Class members had known that Defendants would not secure their Private Information using adequate security, they would not have entrusted Defendants with their Private Information.

161. Plaintiffs and Class members have no adequate remedy at law.

162. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and Class members conferred on it.

163. Defendants 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.

COUNT IV
BREACH OF CONFIDENCE
(On Behalf of the Nationwide Class)

164. Plaintiffs fully incorporate by reference all the above paragraphs, as though fully set forth herein.

165. Plaintiffs and Class members have an interest, both equitable and legal, in the Private Information that was conveyed to and collected, stored, and maintained by Defendants and which was ultimately compromised by unauthorized cybercriminals as a result of the Data Breach.

166. Defendants, in taking possession of this highly sensitive information, have a special relationship with Plaintiffs and the Class. As a result of that special relationship, Defendants were provided with and stored private and valuable information belonging to Plaintiffs and the Class, which Defendants were required by law and industry standards to maintain in confidence.

167. Plaintiffs and the Class provided such Private Information to Defendant under both the express and/or implied agreement of Defendant to limit and/or restrict completely the use and disclosure of such Private Information without Plaintiffs' and Class members' consent.

168. Defendants had a common law duty to maintain the confidentiality of Plaintiffs' and Class members' Private Information.

169. Defendants owed a duty to Plaintiffs and Class members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in Defendants' possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

170. As a result of the parties' relationship of trust, Defendants had possession and knowledge of the confidential Private Information of Plaintiffs and Class members.

171. Plaintiffs' and Class members' Private Information is not generally known to the public and is confidential by nature. Moreover, Plaintiffs and Class members did not consent to nor authorize Defendants to release or disclose their Private Information to unknown criminal actors.

172. Defendants breached the duty of confidence they owed to Plaintiffs and Class members when Plaintiffs' and Class members' Private Information was disclosed to unknown criminal hackers by way of Defendants' own acts and omissions, as alleged herein.

173. Defendants knowingly breached their duties of confidence by failing to safeguard Plaintiffs' and Class members' Private Information, including by, among other things: (a) mismanaging their systems and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of consumer information that resulted in the unauthorized access and compromise of the Private Information; (b) mishandling data security by failing to assess the sufficiency of the safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust their information security programs in light of the circumstances alleged herein; (f) failing to detect the Data Breach at the time it began or within a reasonable time thereafter and give adequate notice to Plaintiffs and Class members thereof; (g) failing to follow their own privacy policies and practices; (h) storing Private Information in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiffs' and Class members' Private Information to a criminal third party.

174. But for Defendants' wrongful breach of confidence owed to Plaintiffs and Class members, their privacy would not have been compromised and their Private Information would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by and/or viewed by unauthorized third parties.

175. As a direct and proximate result of Defendants' breach of confidence, Plaintiffs and Class members have suffered or will suffer injuries, including but not limited to, the

following: loss of their privacy and confidentiality in their Private Information; theft of their Private Information; costs associated with the detection and prevention of fraud and unauthorized use of their Private Information; costs associated with purchasing credit monitoring and identity theft protection services; costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Defendants' Data Breach – including finding fraudulent charges, enrolling in credit monitoring and identity theft protection services, and filing reports with the police and FBI; the imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals; damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others; continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class members' data; and/or mental anguish accompanying the loss of confidence and disclosure of their confidential Private Information.

176. Defendants breached the confidence of Plaintiffs and Class members by making an unauthorized release and disclosure of their confidential Private Information and, accordingly, it would be inequitable for Defendants to retain the benefits they have received at Plaintiffs' and Class members' expense.

177. As a direct and proximate result of Defendants' breach of confidence, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT V
INJUNCTIVE / DECLARATORY RELIEF
(On Behalf of the Nationwide Class)

178. Plaintiffs fully incorporate by reference all the above paragraphs, as though fully

set forth herein.

179. 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. The Court also has broad authority to restrain acts, such as here, that are tortious and violate the terms of the regulations described in this Complaint.

180. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective duties to reasonably safeguard users' Private Information and whether Defendants are maintaining data security measures adequate to protect the Class members, including Plaintiffs, from further data breaches that compromise their Private Information.

181. Plaintiffs allege that Defendants' data-security measures remain inadequate. In addition, Plaintiffs and the Class 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 and fraudulent activity against them will occur in the future.

182. Pursuant to the Court's authority under the Declaratory Judgment Act, Plaintiffs asks the Court to enter a judgment declaring, among other things, the following: (i) Defendants owe a duty to secure individuals' Private Information and to timely notify them of a data breach under the common law and various federal and state statutes; and (ii) Defendants are in breach of these legal duties by failing to employ reasonable measures to secure individuals' Private Information in its possession and control.

183. Plaintiffs further ask the Court to issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry standards to protect individuals' Private Information from future data breaches.

184. If an injunction is not issued, the Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach of Defendants. The risk of another such breach is real, immediate, and substantial. If another breach of Defendants occurs, the Class members will not have an adequate remedy at law because many of the resulting injuries would not be readily quantifiable and Class members will be forced to bring multiple

lawsuits to rectify the same misconduct.

185. The hardship to the Class members if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if a similar data breach occurs again due to the repeated misconduct of Defendants, the Class members will likely be subjected to substantial hacking and phishing attempts, fraud, and other instances of the misuse of their Private Information, in addition to the damages already suffered. On the other hand, the cost to Defendants of complying with an injunction by employing better and more reasonable prospective data security measures is relatively minimal, and Defendants have pre-existing legal obligations to employ such measures.

186. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing additional data breaches of Defendants, thus eliminating the additional injuries that would result to the Class members and the individuals whose personal and confidential information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

a. For an order certifying the proposed Class and appointing Plaintiffs and their counsel to represent the Class;

b. For an order awarding Plaintiffs and Class members actual, statutory, punitive, and/or any other form of damages provided by and pursuant to the statutes cited above;

c. For an order awarding Plaintiffs and Class members restitution, disgorgement and/or other equitable relief provided by and pursuant to the statutes cited above or as the Court deems proper;

d. For an order or orders requiring Defendants to adequately remediate the Breach and its effects.

e. For an order awarding Plaintiffs and Class members pre-judgment and post-judgment interest;

f. For an order awarding Plaintiffs and Class members treble damages, other enhanced damages and attorneys' fees as provided for under the statutes cited above and related statutes;

g. For an order awarding Plaintiffs and the Class members reasonable attorneys' fees and costs of suit, including expert witness fees;

h. For an order awarding such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

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

Dated: December 7, 2023

By: */s/ Nicholas A. Migliaccio*

Nicholas A. Migliaccio
(Maryland Federal Bar No. 29077)
Jason S. Rathod
(Maryland Federal Bar No. 18424)
MIGLIACCIO & RATHOD LLP
412 H Street NE, Ste. 302,
Washington, DC, 20002
Office: (202) 470-3520
nmigliaccio@classlawdc.com
jrathod@classlawdc.com

Attorneys for Plaintiffs and the Proposed Class