UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
FORT LAUDERDALE DIVISION

VIVIAN LINDLEY, individually and on behalf of all others similarly situated, Plaintiff, v. **JERICO PICTURES, INC., D/B/A NATIONAL PUBLIC DATA**, Defendant.	Civil Action No.: 0:24-cv-61622 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Vivian Lindley ("Plaintiff"), individually and on behalf of herself and all others similarly situated, alleges the following against Jerico Pictures, Inc., d/b/a National Public Data ("NPD" or "Defendant"). The following allegations are based upon Plaintiff's personal knowledge with respect to herself and her own acts, and on information and belief as to all other matters.

I. INTRODUCTION

1. Plaintiff and Class Members (defined below) bring this class action against NPD for its failure to properly secure and safeguard Plaintiff's and similarly situated individuals' private information, including but not limited to names, mailing addresses, telephone numbers, email addresses, and Social Security numbers ("Private Information").

2. NPD is a company that specializes in collecting and aggregating public and non-public records for use by businesses to obtain criminal records reports and process employee background checks.

3. This class action is brought on behalf of all citizens of all states in the United States who are the victims of a targeted cyberattack on Defendant that occurred on or before April 8,

2024 ("the Data Breach"), when NDP failed to properly secure and safeguard the Private Information that it collected and maintained as part of its regular business practices.

4. On April 8, 2024, a well-known threat actor, "USDoD," claimed it had stolen 2.9 billion personal records from NPD's website, NationalPublicData.com, and at that time, attempted to sell the data for $3.5 million.[1]

5. Further, on August 6, 2024, another threat actor known as "Fenice" was reported to have leaked the most complete version of the stolen NPD data for free on the "Breached" hacking forum. Reviews of the leaked data estimated that the text files leaked included over 277 gigabytes of and 2.7 billion rows of records.[2]

6. According to analysts who reviewed batches of this unencrypted data, each record consisted of at least the following information: a person's name, mailing addresses, and Social Security numbers.[3]

7. In an August 12, 2024 statement disclosing the security incident on its website, NPD acknowledged the existence of data leaks, but NPD's notice did not describe what kind of data was taken, nor the size and scale of the Data Breach, and specifically, NPD's website failed to provide details on how many people were impacted by the Data Breach.[4]

---

[1] Jennifer Greogry, *National Public Data breach publishes private data of 2.9B US citizens*, SECURITYINTELLIGENCE (Aug. 19, 2024), https://securityintelligence.com/news/national-public-data-breach-publishes-private-data-billions-us-citizens/.

[2] Lawrence Abrams, *Hackers leak 2.7 billion data records with Social Security numbers*, BLEEPING COMPUTER (Aug. 11, 2024), https://www.bleepingcomputer.com/news/security/hackers-leak-27-billion-data-records-with-social-security-numbers/.

[3] Ionut Ilascu, *National Public Data confirms breach exposing Social Security numbers*, BLEEPING COMPUTER (Aug. 16, 2024), https://www.bleepingcomputer.com/news/security/national-public-data-confirms-breach-exposing-social-security-numbers/.

[4] Security Incident, General Information, NATIONAL PUBLIC DATA (Aug. 12, 2024), https://nationalpublicdata.com/Breach.html (last visited Aug. 29, 2024).

8. Defendant knowingly collected the Private Information of customers in confidence, and has a resulting duty to secure, maintain, protect, and safeguard that Private Information against unauthorized access and disclosure through reasonable and adequate security measures.

9. As a result of the Data Breach, Plaintiff and Class Members suffered ascertainable losses, including, but not limited to, a loss of potential value of their private and confidential information, the loss of the benefit of their contractual bargain with Defendant, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

10. Plaintiff and Class Members entrusted their Private Information to Defendant, its officials, and agents, and that Private Information was subsequently compromised, unlawfully accessed, and stolen due to the Data Breach.

11. Plaintiff brings this class action lawsuit on behalf of herself and all others similarly situated to address Defendant's inadequate safeguarding of Plaintiff's and Class Members' Private Information, for failing to provide adequate notice to Plaintiff and other Class Members of the unauthorized access to their Private Information by a cyber attacker, and for failing to provide adequate notice of precisely what information was accessed and stolen.

12. Defendant breached its duties to Plaintiff and Class Members by maintaining Plaintiff's and the Class Members' Private Information in a negligent and reckless manner.

13. Upon information and belief, the means of the Data Breach and potential risk for improper disclosure of Plaintiff's and Class Members' Private Information were known and foreseeable to Defendant. Thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left the Private Information in a dangerous and vulnerable condition.

14. Defendant failed to properly monitor the computer network and systems housing the Private Information.

15. Had Defendant properly monitored its property, it would have discovered the intrusion sooner or been able to prevent it wholly.

16. Exacerbating an already devastating privacy intrusion, Plaintiff's and Class Members' identities are now at a heightened risk of exposure because of Defendant's negligent conduct since the Private Information that Defendant collected and stored is now in the hands of data thieves.

17. Armed with the Private Information accessed in the Data Breach, data thieves can now use the Private Information obtained from Defendant to commit a variety of crimes, including credit/debit card fraud, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

18. As a direct result of the Data Breach, Plaintiff and Class Members have suffered fraud and will continue to be exposed to a heightened and imminent risk of fraud and identity theft, potentially for the rest of their lives. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

19. Plaintiff and Class Members may also incur out-of-pocket costs for purchasing credit monitoring services, credit freezes, credit reports, and other protective measures to deter and detect identity theft.

20. As a direct and proximate result of the Data Breach and subsequent exposure of their Private Information, Plaintiff and Class Members have suffered—and will continue to suffer—damages and economic losses in the form of lost time needed to take appropriate measures to avoid unauthorized and fraudulent charges, putting alerts on their credit files, and dealing with spam phone calls, letters, and emails received as a result of the Data Breach.

21. Plaintiff and Class Members have suffered—and will continue to suffer—an invasion of their property interest in their own Private Information such that they are entitled to damages from Defendant for unauthorized access to, theft of, and misuse of their Private Information.

22. These harms are ongoing, and Plaintiff and Class Members will suffer from future damages associated with the unauthorized use and misuse of their Private Information as thieves will continue to use the information to obtain money and credit in their names for several years.

23. Plaintiff seeks to remedy these harms on behalf of all similarly situated individuals whose Private Information was accessed via and/or compromised by NPD during the Data Breach.

24. Accordingly, Plaintiff brings this action on behalf of herself and all others similarly situated against Defendant, seeking redress for Defendant's unlawful conduct, asserting claims for (a) negligence; (b) negligence *per se*; (c) breach of an implied contract; (d) breach of a third-party beneficiary contract; and (e) unjust enrichment.

II. PARTIES

A. Plaintiff

25. Plaintiff Vivian Lindley ("Lindley") is a resident of Houston, Texas and a citizen of Texas.

B. Defendant

26. Defendant Jerico Pictures, Inc., d/b/a National Public Data ("NPD") is a Florida corporation with its headquarters and principal place of business located at 1801 NW 126th Way, Coral Springs, Florida 33071.

III. JURISDICTION AND VENUE

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

28. This Court has personal jurisdiction over Defendant because NPD's principal place of business is in this District, and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

29. Venue is proper under 18 U.S.C § 1391(b)(1) because NPD resides in this District, a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in, was directed to, and/or emanated from this District, and Defendant conducts substantial business in this District.

IV. STATEMENT OF FACTS

A. Defendant National Public Data's Business

30. NPD is a company that specializes in collecting and aggregating government and public and non-public records for processing criminal background and employee reference checks.

31. Specifically, NPD is a public records data broker that specializes in background checks and fraud prevention, by processing and using bulk data that it has collected on people,

obtained from public record databases, court records, state and national databases, and other data repositories.[5]

32. NPD publicly describes its background check reporting services by stating, "National Public Data.com is a National Information Service provider. We offer nonpublic and public information to carefully screened and certified entities who are legally qualified to receive this information."[6]

B. The Collection of Plaintiff's and Class Members' Private Information is Central to Defendant's Business

33. In exchange for providing its customers, including Plaintiff and Class Members, background check services, Plaintiff and Class Members were required to transfer possession of their Private Information to Defendant, whether knowingly or not.

34. Through the possession and utilization of Plaintiff's and Class Members' Private Information, Defendant assumed duties owed to Plaintiff and Class Members regarding their Private Information.

35. Therefore, Defendant knew or should have known that it was responsible for safeguarding Plaintiff's and Class Members' Private Information from unauthorized access and criminal misuse.

36. Indeed, these duties are expressly assumed and stated by NPD's posted privacy policy which states, "National Public Data is also committed to protecting the personal information we receive about consumers via public and non-public records. We utilize a combination of online

---

[5] *See* Anthony Kimery, *Investigations into massive National Public Data breach heat up*, BIOMETRIC UPDATE (Aug. 27, 2024), https://www.biometricupdate.com/202408/investigations-into-massive-national-public-data-breach-heat-up.

[6] Privacy Policy, General Information, NATIONAL PUBLIC DATA (Aug. 2024), https://nationalpublicdata.com/privacy.html (last accessed Aug. 29, 2024).

and offline security technologies, procedures and organizational measures to help safeguard consumer information against loss, misuse, and unauthorized access, disclosure, alteration and destruction."[7]

37. Plaintiff and Class Members relied on Defendant to keep their Private Information secure and safeguarded for authorized purposes.

38. Defendant owed a duty to Plaintiff and Class Members to secure their Private Information as such, and ultimately Defendant breached that duty.

C. The Data Breach

39. On April 8, 2024, the well-known web-hacking group, "USDoD," claimed it had stolen 2.9 billion personal records from NPD's website, NationalPublicData.com, and at that time, the threat actor attempted to sell the data for $3.5 million.[8]

40. Shortly thereafter, on June 1, 2024, when a portion of these records surfaced on the dark web, security researchers confirmed that many of the leaked records were indeed authentic, sparking widespread concerns about safety, privacy, and potential identity theft resulting from the leak of reported troves of Private Information disclosed in the breach, particularly the possibility of phishing attempts because contact information was ubiquitous in the leak.[9]

41. On July 21, 2024, denizens of the cybercrime community "Breachforums" released more than four terabytes of data they claimed was stolen from NationalPublicData.com.[10] On

---

[7] *Id.*

[8] Gregory, *supra* note 1.

[9] Troy Hunt, *Inside the "3 Billion People" National Public Data Breach*, TROY HUNT (Aug. 14, 2024), https://www.troyhunt.com/inside-the-3-billion-people-national-public-data-breach/.

[10] Brian Krebs, *NationalPublicData.com Hack Exposes a Nation's Data*, KREBS ON SECURITY (Aug. 15, 2024), https://krebsonsecurity.com/2024/08/nationalpublicdata-com-hack-exposes-a-nations-data/.

August 6, 2024, another threat actor known as "Fenice" was reported to have leaked the most complete version of the stolen NPD data for free on the "Breached" hacking forum. Professional reviews of the leaked data estimated that the leaked text files included over 277 gigabytes of and 2.7 billion rows of records.[11]

42. According to analysts who reviewed batches of this data, each record consisted of at least the following information: a person's name, mailing addresses, and Social Security numbers, with some records including additional information, not limited to other names associated with the person, as well as information related to deceased persons, and none of this leaked data was encrypted.[12]

43. Even after the fallout from the NationalPublicData.com breach, researchers discovered that a sister property of NDP, the background search service RecordsCheck.net was hosting an archive that included the source code and plain text usernames and passwords for different components of RecordsCheck.net, which were visually similar to NationalPublicData.com and featured identical login pages. Passwords included in the source code archive were identical to credentials exposed in previous data breaches that involved email accounts belonging to NDP's founder.[13]

44. In an August 12, 2024 statement disclosing the security incident on its website, NPD acknowledged the existence of "leaks of certain data in April 2024 and summer 2024" and suggested that personal records may have been vulnerable months earlier, dating back to an

[11] Abrams, *supra* note 2.

[12] Ilascu, *supra* note 3.

[13] Brian Krebs, *National Public Data Published Its Own Passwords*, KREBS ON SECURITY (Aug. 19, 2024), https://krebsonsecurity.com/2024/08/national-public-data-published-its-own-passwords/.

infiltration associated with a threat actor "that was trying to hack into data in late December 2023."[14] But NPD's notice was woefully deficient in explaining what kind of data was taken, and more so, it was inadequate in describing the size and scale of the Data Breach.[15]

45. Specifically, the notice on NPD's website failed to provide details on how many people were impacted by the Data Breach and when their data was leaked.

46. In an August 10, 2024 filing with the Maine Attorney General's Office, NPD confirmed that the breach began as early as December 2023, and NPD stated that the Data Breach affected 1.3 million people.[16]

47. Following Defendant's realization of the Data Breach, the company failed to provide meaningful notice to Plaintiff and the Class Members. Any notice provided by Defendant failed to include substantive details on the extent of the Data Breach, the software and/or programs exploited in the Data Breach, what subset of customers had what information stolen in the Data Breach, and what steps were taken to mitigate the risk of subsequent cyberattacks and further harm to Plaintiff and the Class Members.

D. Plaintiff's Experiences Following the Data Breach

48. Prior to the breach, Plaintiff Lindley had not used the website NationalPublicData.com. However, on information and belief, Ms. Lindley's non-public and public information was collected and used by NPD for the purposes of furnishing to NPD's clients criminal and employee background reports.

---

[14] NATIONAL PUBLIC DATA, *supra* note 4.

[15] *Id.*

[16] Consumer Information, Data Breach Notifications, MAINE ATT'Y GEN. OFF. (Aug. 10, 2024), https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/25289ca5-a211-4abc-9e29-cbe8d9d5b0e6.html (last visited Aug. 29, 2024).

49. Ms. Lindley received notice of the Data Breach while checking her credit reports and previously purchased identity protection services. This led her to investigate whether her information had been compromised in the National Public Data breach.

50. Ms. Lindley searched her name on websites that host lookup tools frequently used by cybersecurity professionals to determine whether someone was impacted by a breach. Upon entering her information on the online forums "https://npdbreach.com/" and "https://npd.pentester.com/" Ms. Lindley saw on both websites that her Private Information had been leaked in the NPD breach.[17]

51. Thereafter, Ms. Lindley spent time taking action to mitigate the impact of the Data Breach. This effort included checking her bank accounts and other online accounts, changing her passwords, examining her credit score, and researching the potential impact of the Data Breach, all as a result of her Private Information being exposed in the Data Breach.

52. Ms. Lindley intends to spend additional time and effort taking steps to protect her Private Information in the future. Because of the Data Breach, Ms. Lindley spent valuable time attempting to mitigate the harm she otherwise would have spent on other obligations.

53. As a result of the Data Breach, Ms. Lindley has suffered lost time, annoyance, interference, and inconvenience. This is time Ms. Lindley otherwise would have spent performing other activities, such as her job, and/or leisurely activities for the enjoyment of life.

54. As a result of the Data Breach, Ms. Lindley has suffered emotional distress because of the release of her Private Information which she expected Defendant to protect from disclosure, including anxiety, concern, and unease about unauthorized parties viewing, and potentially using her Private Information.

[17] *See* Krebs, *supra* note 12.

55. As a result of the Data Breach, Ms. Lindley will continue to be at heightened risk for financial fraud, medical fraud, and identity theft—and the attendant damages for years to come.

E. Defendant Knew or Should Have Known Both the Value of Private Information and the Risk of Cyberattacks to Those Who Possess Such Private Information

56. At all relevant times, Defendant was well aware that the Private Information they collect from Plaintiff and Class Members is highly sensitive and of significant value to those who would use it for wrongful purposes.

57. Private Information is a valuable commodity to cyber attackers. As the U.S. Federal Trade Commission ("FTC") recognizes, identity thieves can use this information to commit an array of crimes including identify theft and medical or financial fraud.[18] Indeed, a robust "cyber black market" exists in which criminals openly post stolen Private Information on multiple underground websites, commonly referred to as the dark web.

58. The number of U.S. data breaches surpassed 1,000 in 2016, a record high and a forty percent increase in the number of data breaches from the previous year.[19] In 2022, 1,802 data compromises were reported that impacted over 422 million victims—marking a 42% increase in the number of victims impacted since 2021.[20] That upward trend continues.

---

[18] *What to Know About Identify Theft*, FED. TRADE COMM'N, https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Aug. 27, 2024).

[19] Press Release, CyberScout, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (Jan. 19, 2017), https://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208.html.

[20] 2022 Data Breach Report, IDENTITY THEFT RES. CTR. (Jan. 2023), https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC_2022-Data-Breach-Report_Final-1.pdf.

59. The ramifications of Defendant's failures to keep Plaintiff's and Class Members' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Fraudulent activity might not show up for six to twelve months or even longer.

60. Further, criminals often trade stolen Private Information on the "cyber black-market" for years following a breach. Cybercriminals can post stolen Private Information on the internet, thereby making such information publicly available, giving data thieves ample time to fraudulently use the victim's name.

61. As entities serving consumers in the background check information space, Defendant knew, or reasonably should have known, the importance of safeguarding Plaintiff's and Class Members' Private Information entrusted to it, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

F. Defendant Failed to Comply with FTC Guidelines

62. Defendant was also prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA") 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 consumers' sensitive personal information is an "unfair practice" in violation of the FTCA.[21]

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

63. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[22]

64. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[23] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct any security problems.

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

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

---

[22] *Start With Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

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

67. Defendant failed to properly implement basic data security practices. Defendant's failures to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA. 15 U.S.C. § 45.

68. Defendant was fully aware of their obligations to protect the Private Information of Plaintiff and Class Members because of their positions as entities whose businesses center on contractual relationships with their clients and necessary collection, storage, and safeguarding of Private Information as a result of those contractual relationships. Defendant was also aware of the significant repercussions that would result from their failures to make good on those obligations.

G. Cyber Criminals Have and Will Continue to Use Plaintiff's and Class Members' Private Information for Nefarious Purposes

69. Plaintiff's and Class Members' Private Information is of great value to cybercriminals, and the data stolen in the Data Breach can be used in a variety of ways by criminals to exploit Plaintiff and Class Members and to profit off their misfortune and stolen information. The cybercriminals' motives for the Data Breach were purely nefarious and malicious in nature: their one goal was to access Defendant's systems to obtain valuable Private Information to sell on the dark web.

70. Private Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.

71. These risks are both certainly impending and substantial. As the FTC has reported, if cyber thieves get access to personally identifiable information, they will use it.[24]

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

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[25]

73. If cyber criminals manage to access financial information, health insurance information, and other personally sensitive data using the Private Information compromised in the Data Breach, there is no limit to the amount of fraud to which Defendant may have exposed the Plaintiff and Class Members.

H. Plaintiff and Class Members Suffered Damages

74. The ramifications of Defendant's failures to keep Plaintiff's and Class Members' Private Information secure are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.[26]

75. In addition to their obligations under state laws and regulations, Defendant owed a common law duty to Plaintiff and Class Members to protect Private Information entrusted to it,

---

[24] Ari Lazarus, *How fast will identity thieves use stolen info?*, MILITARY CONSUMER (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info (last visited Aug. 27, 2024).

[25] U.S. Gov't Accountability Off., GAO-07-737, *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (2007), https://www.gao.gov/assets/a262904.html.

[26] *2014 LexisNexis True Cost of Fraud Study*, LEXISNEXIS (Aug. 2014), https://web.archive.org/web/20190331095639/https://www.lexisnexis.com/risk/downloads/assets/true-cost-fraud-2014.pdf (last visited Aug. 29, 2024).

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.

76. Defendant further owed and breached their duties to Plaintiff and Class Members to implement processes and specifications that would detect a breach of their security systems in a timely manner and to timely act upon warnings and alerts, including those generated by their own security systems.

77. As a direct result of Defendant's intentional, willful, reckless, and negligent conduct which resulted in the Data Breach, cyber thieves were able to access, acquire, view, publicize, and/or otherwise cause the misuse and/or identity theft of Plaintiff's and Class Members' Private Information as detailed above, and Plaintiff and Class Members are now at a heightened risk of identity theft and fraud.

78. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many days repairing damage to their good name and credit record. Some consumers 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.

79. Other risks of identity theft include loans opened in the name of the victim, medical services billed in their name, utility bills opened in their name, tax return fraud, and credit card fraud.

80. As a result of the Data Breach, Plaintiff's and Class Members' Private Information has diminished in value.

81. The Private Information belonging to Plaintiff and Class Members is personal, private in nature, and was left inadequately protected by Defendant who did not obtain Plaintiff's or Class Members' consent to disclose such Private Information to any other person as required by applicable law and industry standards.

82. The Data Breach was a direct and proximate result of Defendant's failures to: (a) properly safeguard and protect Plaintiff's 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's and Class Members' Private Information; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

83. Defendant had the resources necessary to prevent the Data Breach, but neglected to adequately implement data security measures, despite its obligations to protect such data.

84. Had Defendant remedied the deficiencies in its data security systems and adopted security measures recommended by experts in the field, it would have prevented intrusions into Defendant's systems and, ultimately, the theft of Plaintiff's and Class Members' Private Information.

85. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing and increased risk of harm from identity theft and fraud, requiring Plaintiff and Class Members 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.

86. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "[r]esolving the problems caused by identity theft [could] take more than a year for some victims."[27]

87. Defendant's failures to adequately protect Plaintiff's and Class Members' Private Information has resulted in Plaintiff 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. Rather than assist those affected by the Data Breach, Defendant is putting the burden on Plaintiff and Class Members to discover possible fraudulent activity and identity theft.

88. As a result of Defendant's failures to prevent the Data Breach, Plaintiff and Class Members have suffered, will suffer, and are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of their Private Information;

b. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

c. 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

[27] Erika Harrell & Lynn Langton, *Victims of Identity Theft, 2012*, U.S. DEP'T OF JUST., OFF. OF JUSTICE PROGRAMS BUREAU OF JUSTICE STATISTICS (Dec. 2013), https://web.archive.org/web/20200207180624/https://www.bjs.gov/content/pub/pdf/vit12.pdf.

researching how to prevent, detect, contest, and recover from identity theft and fraud;

d. The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the Private Information in its possession;

e. 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 Plaintiff and Class Members; and

f. Anxiety and distress resulting from fear of misuse of their Private Information.

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

V. CLASS ACTION ALLEGATIONS

90. Plaintiff brings this class action on behalf of herself and all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

91. The class (the "Class") that Plaintiff seeks to represent is defined as follows, subject to amendment as appropriate:

> **All individuals in the United States whose Private Information was compromised as a result of the Data Breach by National Public Data.**

92. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers, and directors, current or former employees, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state, or local governments, including but not limited to its departments, agencies,

divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as its immediate family members.

93. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

94. Numerosity, Fed R. Civ. P. 23(a)(1): The Class is so numerous that joinder of all members of the class ("Class Members") is impracticable. Defendant publicly identified at least 1.3 million individuals whose Private Information may have been improperly accessed and compromised in the Data Breach.

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

a. Whether and when Defendant actually learned of the Data Breach and whether its response was adequate;

b. Whether Defendant owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining Class Members' Private Information;

c. Whether Defendant breached that duty;

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and Class Members' Private Information;

e. Whether Defendant acted negligently in connection with the monitoring and/or protecting of Plaintiff's and Class Members' Private Information;

f. Whether Defendant knew or should have known that they did not employ reasonable measures to keep Plaintiff's and Class Members' Private Information secure and prevent loss or misuse of that Private Information; and

g. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendant caused Plaintiff's and Class Members' damages;

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

j. Whether Plaintiff and the other Class Members are entitled to actual damages, extended credit monitoring, and other monetary relief;

k. Whether Defendant violated common law and statutory claims alleged herein.

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

97. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect the Class uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

98. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that she has no disabling conflicts of interest that

would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to Class Members and the infringement of the rights and the damages she has suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex consumer class action litigation, and Plaintiff intends to prosecute this action vigorously.

99. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a corporation, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

100. The nature of this action and the nature of laws available to Plaintiff and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and the Class for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since Defendant would be able to exploit and overwhelm the limited resources of the Class with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and

individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

101. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

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

103. Unless a Class-wide injunction is issued, Plaintiff and Class Members remain at risk that Defendant will continue to fail to properly secure the Private Information of Plaintiff and Class Members resulting in another data breach, continue to refuse to provide proper notification to Class Members regarding the Data Breach, and continue to act unlawfully as set forth in this Class Action Complaint.

104. Defendant acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

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

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

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

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

e. Whether Class Members are entitled to actual damages, additional credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

VI. CLAIMS

COUNT I

Negligence
(On Behalf of Plaintiff and the Class against Defendant)

106. Plaintiff repeats and realleges all allegations set forth above as if they were fully set forth herein.

107. Plaintiff and Class Members' Private Information was used by Defendant in order to provide public record and background check services.

108. Defendant knew, or should have known, of the risks inherent in collecting and storing the Private Information of Plaintiff and Class Members.

109. As described above, Defendant owed duties of care to Plaintiff and Class Members whose Private Information had been entrusted with Defendant.

110. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

111. Defendant acted with wanton disregard for the security of Plaintiff's and Class Members' Private Information. Defendant knew or reasonably should have known that it had inadequate data security practices to safeguard such information, and Defendant knew or reasonably should have known that data thieves were attempting to access databases containing Private Information and personally identifiable information (or "PII"), such as those of Defendant.

112. A "special relationship" exists between Defendant and Plaintiff and Class Members. Defendant entered into a "special relationship" with Plaintiff and Class Members because Defendant collected the Private Information of Plaintiff and the Class Members—information that Plaintiff and the Class Members often did not know Defendant was collecting and publishing in order to conduct its background check services.

113. But for Defendant's wrongful and negligent breaches of the duties owed to Plaintiff and the Class Members, Plaintiff and the Class Members would not have been injured.

114. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breaches of its duties. Defendant knew or reasonably should have known it was failing to meet its duties, and that Defendant's breaches of such duties would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

115. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II

Negligence *Per Se*
(On Behalf of Plaintiff and the Class against Defendant)

116. Plaintiff repeats and realleges all allegations set forth above as if they were fully set forth herein.

117. Pursuant to the FTCA (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

118. Defendant breached its duties to Plaintiff and Class Members under the FTCA (15 U.S.C. § 45) by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

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

120. But for Defendant's wrongful and negligent breaches of their duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

121. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breaches of its duties. Defendant knew or reasonably should have known that it was failing to meet their duties, and that Defendant's breaches would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

122. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III

Breach of Implied Contract
(On Behalf of Plaintiff and the Class against Defendant)

123. Plaintiff repeats and realleges all allegations set forth above as if they were fully set forth herein.

124. Plaintiff and Class Members entered into an implied contract with Defendant when Defendant used Plaintiff's and Class Members' Private Information to conduct and furnish background check services and reports to Defendant's customers. The Private Information provided by Plaintiff and Class Members to Defendant was governed by and subject to Defendant's privacy duties and policies.

125. Defendant agreed to safeguard and protect the Private Information of Plaintiff and Class Members and to timely and accurately notify Plaintiff and Class Members in the event that their Private Information was breached or otherwise compromised.

126. Plaintiff and Class Members entered into the implied contracts with the reasonable expectation that Defendant's data security practices and policies were reasonable and consistent with industry standards. Plaintiff and Class Members believed that Defendant would use part of the monies paid to Defendant under the implied contracts to fund adequate and reasonable data security practices.

127. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract or implied terms between Plaintiff and Class Members and Defendant. The safeguarding of the Private Information of Plaintiff and Class Members and prompt and sufficient notification of a breach involving Private Information was critical to realize the intent of the parties.

128. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

129. Defendant breached its implied contracts with Plaintiff and Class Members to protect Plaintiff's and Class Members' Private Information when they: (a) failed to have security protocols and measures in place to protect that information; (b) disclosed that information to unauthorized third parties; and (3) failed to provide sufficient notice that their Private Information was compromised as a result of the Data Breach.

130. As a direct and proximate result of Defendant's breaches of implied contract, Plaintiff and Class Members have suffered damages.

COUNT IV

Breach of Third-Party Beneficiary Contract
(On behalf of Plaintiff and the Class against Defendant)

131. Plaintiff repeats and realleges all allegations set forth above as if they were fully set forth herein.

132. This Count is pleaded in the alternative to the breach of implied contract claim above (Count III).

133. Upon information and belief, Defendant entered into contracts with its clients, to provide background check and information services—using the Private Information of Plaintiff and Class Members.

134. Upon information and belief, Plaintiffs and Class Members were the express, foreseeable, and intended beneficiaries of valid and enforceable contracts between Defendant and its customers that, upon information and belief, include obligations to keep sensitive PII private and secure.

135. Upon information and belief, these contracts included promises made by Defendant that expressed and/or manifested intent that they were made primarily and directly to benefit Plaintiffs and Class Members and safeguard the PII entrusted to Defendant in the process of providing these services.

136. These contracts were made for the benefit of Plaintiff and Class Members given the transfer of their Private Information to Defendant for storage, protection, and safeguarding was the objective of the contracting parties. Therefore, Plaintiff and Class Members were direct and express beneficiaries of these contracts.

137. Defendant knew that a breach of these contracts with its clients would harm Plaintiff and Class Members.

138. Defendant breached the contracts with its clients when it failed to utilize adequate computer systems or data security practices to safeguard Plaintiff's and Class Members' Private Information.

139. Plaintiff and Class Members were harmed by Defendant's breaches in failing to use reasonable security measures to safely store and protect Plaintiff's and Class Members' Private Information.

140. Plaintiff and Class Members are therefore entitled to damages in an amount to be determined at trial.

COUNT V

Unjust Enrichment
(On Behalf of Plaintiff and the Class against Defendant)

141. Plaintiff repeats and realleges all allegations set forth above as if they were fully set forth herein.

142. This Count is pleaded in the alternative to the breach of implied contract claim above (Count III) and the breach of third-party beneficiary claim above (Count IV).

143. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their Private Information—Private Information that has inherent value. In exchange, Plaintiff and Class Members should have been entitled to Defendant's adequate storage and safeguarding of their Private Information.

144. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and Class Members.

145. Defendant profited from Plaintiff's and Class Members' retained Private Information and used their Private Information for business purposes.

146. Defendant failed to store and safeguard Plaintiff's and Class Members' Private Information. Thus, Defendant did not fully compensate Plaintiff and Class Members for the value of their Private Information.

147. As a result of Defendant's failures, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between the healthcare services with the reasonable data privacy and security practices and procedures that Plaintiff and Class Members paid for, and the inadequate healthcare services without reasonable data privacy and security practices and procedures that they received.

148. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to implement—or adequately implement—the data privacy and security practices and procedures that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state and local laws, and industry standards.

149. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds received by Defendant.

150. A constructive trust should be imposed upon all unlawful or inequitable sums received by Defendant traceable to Plaintiff and Class Members.

VII. PRAYER FOR RELIEF

A. That the Court certify this action as a class action and certify the Class as proper and maintainable pursuant to Rule 23 of the Federal Rules of Civil Procedure; declare that Plaintiff is the proper class representative; and appoint Plaintiff's Counsel as Class counsel;

B. That the Court grant permanent injunctive relief to prohibit Defendant from engaging in the unlawful acts, omissions, and practices described herein;

C. That the Court award Plaintiff and Class Members compensatory, consequential, and general damages in an amount to be determined at trial;

D. That the Court order disgorgement and restitution of all earnings, profits, compensation, and benefits received by Defendant as a result of its unlawful acts, omissions, and practices;

E. That the Court award statutory damages, trebled, and punitive or exemplary damages, to the extent permitted by law;

F. That Plaintiff be granted the declaratory relief sought herein;

G. That the Court award to Plaintiff the costs and disbursements of the action, along with reasonable attorneys' fees, costs, and expenses;

H. That the Court award pre- and post-judgment interest at the maximum legal rate; and

I. That the Court grant all such other relief as it deems just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury.

Dated: August 30, 2024

Respectfully submitted,

/s/ Jay Eng
Jay Eng (FL. Bar No. 146676)

BERMAN TABACCO
Patrick T. Egan (*pro hac vice forthcoming*)
One Liberty Square
Boston, MA 02109
Telephone: (617) 542-8300
jeng@bermantabacco.com
pegan@bermantabacco.com

Pierce H. Stanley (*pro hac vice forthcoming*)
425 California Street, Suite 2300
San Francisco, CA 94104
Telephone: (415) 433-3200
pstanley@bermantabacco.com

Counsel for Plaintiff Vivian Lindley and the Putative Class