UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

George D., *individually and as legal guardian of his minor child G.D., individually and on behalf of others similarly situated,* Plaintiff, v. PEARSON, plc, d/b/a Pearson Clinical Assessments; and NCS PEARSON, INC., Defendants.	**Case No. 0:19-cv-2814** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff, George D., individually, and as legal guardian for his minor child G.D., on behalf of all others similarly situated ("Plaintiff"), brings this action against Defendants, PEARSON, plc, d/b/a Pearson Clinical Assessments ("Pplc") and NCS PEARSON, INC., ("NCSP") (collectively, "Pearson" or "Defendants") to obtain damages, restitution, and injunctive relief for the Classes, as defined below, from Defendants. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record:

NATURE OF THE ACTION

1. This action is brought, in part, for the protection of our most vulnerable, our student children. Plaintiff brings this class action against Defendants for failing to secure and safeguard the personally identifiable information (referred to interchangeably as "PII" or "Private Information") that Pearson collected, maintained, and stored in its AIMSweb 1.0 platform ("AIMSweb"), and for failing to provide timely and adequate notice to Plaintiff and other Class members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed (the "Data Breach").

2. Due to Defendants' negligence, the PII that it collected and maintained is now in the hands of thieves. Accordingly, Plaintiff brings this action against Defendants seeking redress for their unlawful conduct asserting claims for: (i) negligence; (ii) breach of express contract; (iii) breach of implied contract; (iv) intrusion upon seclusion.

3. Plaintiff seeks to recover damages, equitable relief, including injunctive relief, restitution, disgorgement, reasonable costs and attorney fees, and all other remedies this Court deems proper.

PARTIES

4. Plaintiff, George D., individually and as legal guardian for his minor child, G.D., is and was at all times mentioned herein, an individual citizen of the State of Georgia, residing in Rome, Georgia. G.D. attended school in Rome, Georgia. G.D.'s PII was stolen in connection with the Data Breach. Like other class members, G.D. suffered harms as a result of the Data Breach, including, but not limited to, (i) the theft of her PII;

(ii) the time and costs associated with dealing with the Data Breach, such as the prevention of future identity theft and the inconvenience, nuisance, and annoyance of dealing with all other issues resulting from the Data Breach; (iii) the imminent heightened risk of identity theft; (iii) invasion of her privacy; and (iv) damage to and diminution in value of the PII that Defendants failed to safeguard.

5. Defendant, Pplc, is a British multinational publishing and education company headquartered in London England. Plpc does business throughout the United States with its principal place of business in San Antonio, Texas.

6. Defendant, NCSP, is a Minnesota corporation and a wholly owned subsidiary of Pearson, plc with NCSP's principal executive office being in Bloomington, Minnesota.

JURISDICTION AND VENUE

7. Jurisdiction is proper in this Court pursuant to 28 U.S.C. §1332(d)(2) because diversity of citizenship exists between the parties to this action, the aggregate amount in controversy, exclusive of interests and costs, exceeds $5 million, and there are greater than 100 members of the proposed class.

8. This Court has personal jurisdiction over Defendants because they are authorized to do business in this District and regularly conduct business in this District, have sufficient minimum contacts with this state, and/or sufficiently avail themselves of the markets of this state through their promotion, sales, licensing and marketing within this state.

9. Pursuant to 28 U.S.C. §1391(b)(1) & (2), venue is proper in this District because NCSP resides in this district and substantial portions of the acts and transactions complained of occurred in this District.

DEFENDANTS' BUSINESS OPERATIONS

10. Defendant Pplc is a British Corporation with its principal place of business in San Antonio, Texas with accounts spanning schools and universities across all 50 States. Pplc, the world's largest education publisher, operates in 70 different countries, has over 24,000 employees, and has total assets exceeding $9 billion. Pplc provides education and assessment tools, content, product, and services designed to help learners at all stages of their education.

11. At all relevant times, Pplc did business under the trade name Pearson Clinical Assessment ("PCA"). PCA was responsible for AIMSweb.

12. AIMSweb is an online progress monitoring system based on direct, frequent, and continuous student assessment. Using AIMSweb, results from monitoring are reported to students, parents, teachers, and administrators via a web-based data management and reporting system to determine response to instruction.

13. Defendant NCSP is a Minnesota public corporation based in Bloomington, Minnesota with over 6,000 employees. NCSP provides learning material, assessment, and digital services to schools, colleges, and universities and markets application software for education, testing, assessment, and complex data management. NCSP was primarily responsible for the AIMSweb progress monitoring system.

THE DATA BREACH

14. The Data Breach occurred as a result of Defendants' failure to secure and protect Plaintiff and Class members' PII.

15. AIMSweb systems were licensed to various schools and school districts by Defendants.

16. Plaintiff and Class members utilizing the AIMSweb system, as required by their schools' curricula, were required to provide Defendants with valuable and sensitive PII, including their first and last names, dates of birth, email addresses, and unique identification numbers.

17. Plaintiff and Class members relied on Defendants to keep their PII confidential and secure, to be used solely for education purposes, and to protect against unauthorized disclosure of the PII.

18. Defendants' online Privacy Notice promises that consumers should "expect information to be treated with total confidentiality," that Pearson takes "full responsibility for the information [they] hold about you" and acknowledges an awareness of and the obligation to "comply with all relevant data protection laws."[1]

19. In mid-March 2019, Pearson learned from the FBI of a cyberattack that had occurred in November 2018 which allowed the perpetrator unauthorized access to over 13,000 school and university accounts on the AIMSweb student monitoring and

[1] https://www.pearson.com/corporate/privacy-notice.html

assessment platform, i.e., the Data Breach.[2] Each account varied in size and could potentially contain the information for thousands of students.

20. The FBI is aware of, and has warned that, the growth of education technologies and collection of student data can have privacy and safety implications if compromised. Among other problems, this can result in the targeting of children for bullying, tracking, social engineering, and identify theft.[3]

21. The data affected by the Data Breach included, but was not limited to, students' first and last names, dates of birth, and email addresses.

22. According to Pearson spokesman, Scott Overland, Pearson could not confirm that the students' information had not been misused, apologized to the affected students and their parents, and noted that Pearson was "offering complementary credit monitoring services as a precautionary measure."[4]

23. Ironically, after the Data Breach, Mr. Overland claimed "[p]rotecting our customer's information is of critical importance to us."[5] Yet, Pearson refused to offer credit monitoring services until four months after it learned of the Data Breach and nearly nine months after it had occurred, thus preventing victims from protecting their PII.[6]

[2] *See, e.g.*, Ex. 1, July 19, 2019 letter from Pearson to Floyd County Board of Education.
[3] https://www.ic3.gov/media/2018/180913.aspx
[4] https://www.chalkbeat.org/posts/co/2019/08/29/pearson-data-breach-revives-concerns-about-student-privacy-in-colorado/
[5] https://www.chalkbeat.org/posts/co/2019/08/29/pearson-data-breach-revives-concerns-about-student-privacy-in-colorado/
[6] http://www.northwestgeorgianews.com/rome/news/local/contractor-notifies-fcs-of-data-security-incident/article_18c6bcfc-beea-11e9-ab6c-9b0f5c9a819e.html

24. What's more, Pearson did not bother to notify students or parents directly, but rather left that sordid task to the various schools and school districts, again, belying their "critical" concern and the overall risks inherent with the additional passage of time.[7]

25. Pearson failed to appreciate the gravity of the Data Breach which, according to the Identity Theft Resource Center, heightened the risk that additional damage might follow the Data Breach, including the possibility that hackers and thieves would target students' other retail, social media, and work-related accounts.[8]

26. Following the Data Breach notification, individual school boards notified their students and parents in the manner they each saw fit.[9]

27. According to Pearson's notices to the schools and school districts, Pearson was still undergoing reviews to determine what additional steps were necessary to protect the safety and security of students' PII.[10]

28. Whether through its systems—which were plainly in need of enhancement, based on the existence of the Data Breach and Pearson's failure to discover it—or its reckless and intentional delay in notification, Pearson negligently and unlawfully failed to safeguard students' PII and failed to timely notify them when it was compromised.

---

[7] http://www.northwestgeorgianews.com/rome/news/local/contractor-notifies-fcs-of-data-security-incident/article_18c6bcfc-beea-11e9-ab6c-9b0f5c9a819e.html; *See e.g.* Ex. 1, July 19, 2019 letter from Pearson to Floyd County Board of Education.

[8] https://www.idtheftcenter.org/students-and-schools-affected-by-pearson-data-breach/

[9] *See, e.g.*, Ex. 1, July 19, 2019 letter from Pearson to Floyd County Board of Education; https://www.floydboe.net/site/default.aspx?PageType=3&DomainID=4&ModuleInstanceID=29&ViewID=6446EE88-D30C-497E-9316-3F8874B3E108&RenderLoc=0&FlexDataID=7530&PageID=1&fbclid=IwAR1PvOy_qXzMiUCwuec-pvZReDhPBFLEAgsScYlS7j8FtGfngYTfHIH9A90

[10] *See, e.g.*, Ex. 1, July 19, 2019 letter from Pearson to Floyd County Board of Education.

29. Accordingly, students, including Plaintiff, now face an increased risk of fraud, identity theft, bullying, shaming, social engineering, tracking, or other means of targeting.

30. According to Arkose Labs, a leading security fraud and abuse prevention organization, the Pearson Data Breach is significant because it "exposed sensitive personal identifiable information (PII) on hundreds of thousands of school and university students and the attack went unnoticed by Pearson for months."[11]

31. Pearson's customers, a younger demographic, "are inherently more vulnerable because they have more at stake in the long-term and that criminals will be able to immediately leverage the exposed email addresses to carry out credential stuffing attacks against other organizations."[12]

32. "[T]he breach tarnishes a younger demographic's digital footprint on the dark web at an early age and gives cybercriminals a long runway to continue collecting additional information on these students by sharing it on the dark web's connected ecosystem for the rest of their lives".

[11] https://www.scmagazine.com/home/security-news/data-breach/pearson-data-breach-involves-thousands-of-university-accounts/

[12] https://www.scmagazine.com/home/security-news/data-breach/pearson-data-breach-involves-thousands-of-university-accounts/

DATA BREACHES PUT STUDENTS AT AN INCREASED RISK OF FRAUD, IDENTIFY THEFT, AND OTHER TARGETING

33. In September 2018, the FBI issued a Public Service Announcement specifically addressing the type of data breach that has happened in this instance due to the growth of education technologies.[13]

34. The FBI identified some of the potential data that could be compromised as PII; biometric data; academic progress; behavioral, disciplinary, and medical information; Web browsing history; students' geolocation; IP addresses used by students; and classroom activities.[14]

35. This collection of data can present "unique exploitation opportunities for criminals" to extort and threaten students for release of additional personal information.[15]

36. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GOA Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[16]

37. The Federal Trade Commission recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (it recommends that people consider an extended fraud alert that lasts for 7 years if someone steals their

[13] https://www.ic3.gov/media/2018/180913.aspx
[14] https://www.ic3.gov/media/2018/180913.aspx
[15] https://www.ic3.gov/media/2018/180913.aspx
[16] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 12, 2019) ("GAO Report").

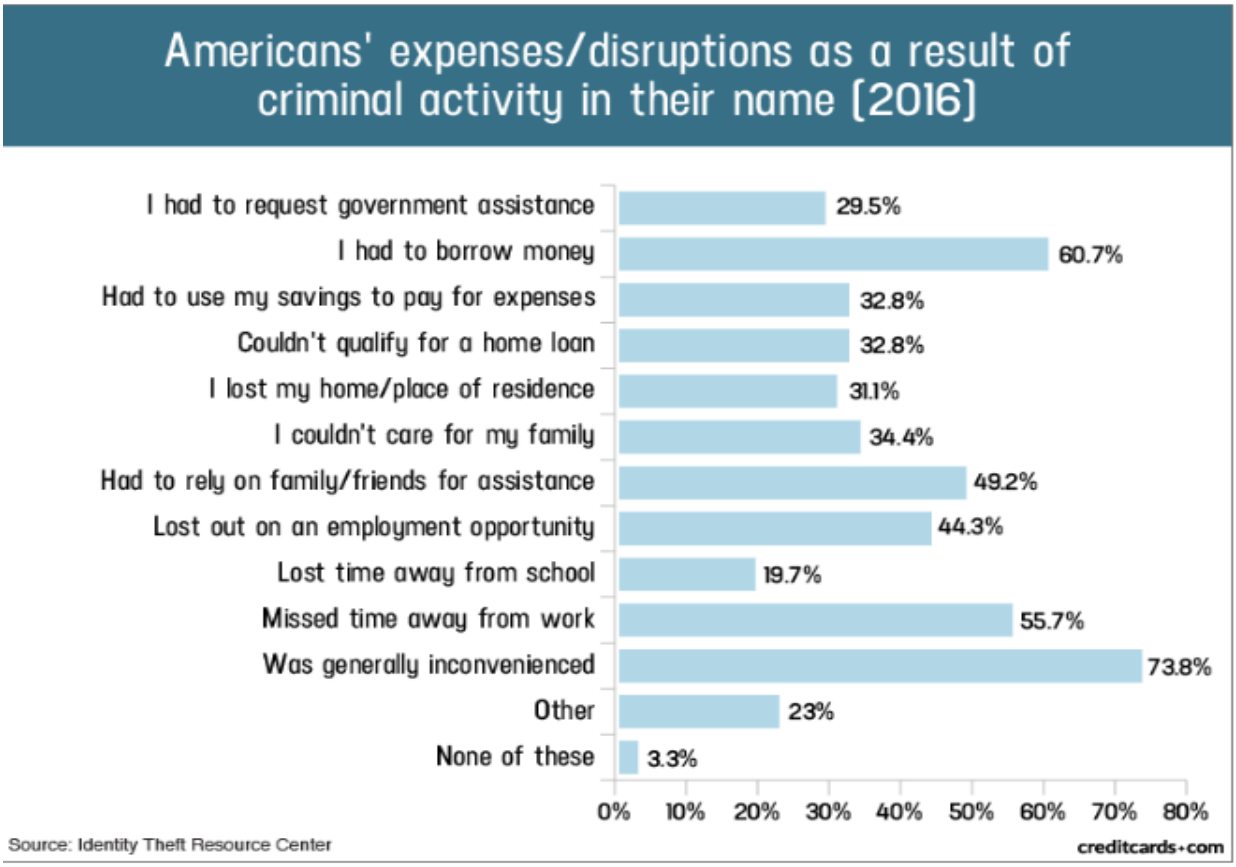
identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[17]

38. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

39. Identity thieves can also use such PII to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and related information to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's PII, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

40. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of PII[18]:

[17] *See* https://www.identitytheft.gov/Steps (last visited April 12, 2019).
[18] Source: "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited October 24, 2019).



41. What's more, theft of PII is also gravely serious. PII is a valuable property right.[19] Its value is reflected in the value placed on "big data" by corporate America. It is further highlighted by the repeated efforts to engage in cyber thefts, the consequences of which include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

42. It must also be noted there may be a time lag between when harm occurs versus when it is discovered, and also between when PII and/or financial information is

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

stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

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

See GAO Report, at p. 29.

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

44. Thus, there is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class members are at an increased risk of fraud and identity theft for many years into the future.

PLAINTIFF AND CLASS MEMBERS' DAMAGES

45. As a direct and proximate result of Defendants' conduct, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud, identity theft, bullying, tracking, extortion, social engineering, shaming, threatening, and other targeting.

46. Plaintiff and Class members have suffered or will suffer actual injury as a direct result of the Data Breach, including but not limited to the following harms: (i) the theft of their PII; (ii) the time and costs associated with dealing with the Data Breach,

such as the prevention of future identity theft and the inconvenience, nuisance, and annoyance of dealing with all other issues resulting from the Data Breach; (iii) the imminent heightened risk of identity theft; (iii) invasion of their privacy; and (iv) damage to and diminution in value of their PII that Defendants failed to safeguard. In addition, many victims suffer ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing “freezes” and “alerts” with credit reporting agencies;

g. Spending time on the phone with or at the financial institution to dispute fraudulent charges;

h. Contacting their financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled;

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come;

l. Obtaining new student identification numbers; and

m. Changing email addresses and account passwords.

47. Moreover, Plaintiff and Class members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

48. As a result of Defendants' misconduct, the Data Breach has made Plaintiff's and Class members' PII available to criminals for misuse. The Data Breach directly resulted in injuries such as: theft of personal information; costs of identity theft detection and further protection; costs to mitigate the future consequences of the Data Breach, including but not limited to, time taken from life enjoyment, inconvenience, nuisance, and annoyance; impending injury resulting from fraud and identify theft due to PII for sale on the dark web; diminution of value of PII; and loss of privacy.

49. Further, as a result of Defendants' conduct, Plaintiff and Class members are forced to live with the anxiety that their private health information—which contains the

most intimate details about a person's life, including what ailments they suffer, whether physical or mental—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

50. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and Class members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

CLASS ACTION ALLEGATIONS

51. Plaintiff seeks class certification of the classes and subclass set forth herein pursuant to Federal Rules of Civil Procedure 23(b)(2) and (b)(3).

52. Plaintiff proposes the following class definition for a nationwide class, subject to amendment as appropriate, with a class defined as follows:

> **The Nationwide Class**: All individuals residing in the United States whose Private Information was received, gathered, shared, obtained, or otherwise found itself in the possession of Defendants and compromised in the Data Breach. Excluded from the Class are Defendants' officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff (the "Nationwide Class").

53. Plaintiff proposes the following state subclass definition, subject to amendment as appropriate, with a class defined as follows:

> **The Georgia Subclass**: All individuals residing in the State of Georgia whose Private Information was received, gathered, shared, obtained, or otherwise found itself in the possession of Defendants and compromised in the Data Breach. Excluded from the Class are Defendants' officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of

the judiciary to whom this case is assigned, their families and members of their staff (the "Georgia Subclass").

54. Plaintiff seeks class certification of claims for the common law privacy cause of action, "Intrusion Upon Seclusion" on behalf of a multi-state class, subject to amendment as appropriate, with a class defined as follows:

> **The Multi-state Class**: All individuals residing in the states of Alabama, Arizona, California, Connecticut, Delaware, Florida, Georgia, Illinois, Kentucky, Louisiana, Massachusetts, Michigan, Minnesota, Mississippi, Nevada, New York, North Carolina, Ohio, Pennsylvania, Texas, Vermont, Virginia, and Wisconsin whose Private Information was received, gatherer, shared, obtained, or otherwise found itself in the possession of Defendants and compromised in the Data Breach. Excluded from the Class are Defendants' officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff (the "Multi-state Class").

55. Numerosity. The members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of Class members is unknown to Plaintiff at this time, based on information and belief, the Class is in the hundreds of thousands of students.

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

a) Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff and Class members' Private Information;

b) Whether Defendants recklessly delayed or knowingly concealed notification to affected consumers of the Data Breach

c) Whether Defendants unreasonably delayed in notifying affected consumers of the Data Breach and whether the belated notice was adequate;

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

e) Whether Defendants' conduct was negligent;

f) Whether Defendants' acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

g) Whether Defendants breached express and/or implied contracts with Plaintiff and Class members;

h) Whether Plaintiff and Class members are entitled to damages and/or injunctive relief.

57. Typicality. Plaintiff's claims are typical of those of other Class members because Plaintiff's information, like that of every other Class member, was misused, and/or disclosed by Defendants.

58. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiff's Counsel are competent and experienced in litigating class actions.

59. Superiority of Class Action. A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all Class members is impracticable. Furthermore, the adjudication of this controversy

through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

60. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendants' violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Classes.

61. Defendants have acted or refused to act on grounds that apply generally to the Class, as alleged above, such that certification is proper under FRCP 23(b)(2).

CAUSES OF ACTION

FIRST COUNT
Negligence
(On Behalf of Plaintiff and the Nationwide and Georgia Classes)

62. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

63. Defendants knowingly collected, came into possession of, and maintained Plaintiff and Class members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

64. Defendants had, and continue to have, a duty to timely disclose that Plaintiff and Class members' Private Information within their possession was compromised and precisely the type(s) of information that were compromised.

65. Defendants had a duty to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff and Class members' Private Information.

66. Defendants' duties arose from the relationship to Plaintiff and Class members due to Defendants' custody and possession of PII, from industry custom and standards, and from Defendants' Privacy Notice.

67. Defendants systematically failed to provide adequate security for data in their possession.

68. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding Plaintiff and Class members' Private Information within Defendants' possession.

69. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class members by failing to implement or adhere to standard industry protocols.

70. Defendants, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff and Class members' Private Information.

71. Defendants, through their actions and/or omissions, unlawfully breached their duty to timely disclose to Plaintiff and Class members that the Private Information within Defendants' possession might have been compromised and precisely the type of information compromised.

72. Defendants' breach of duties owed to Plaintiff and Class members caused Plaintiff and Class members' Private Information to be compromised.

73. As a result of Defendants' ongoing failure to notify Plaintiff and Class members regarding specifically what type of Private Information has been compromised, Plaintiff and Class members are unable to take the necessary precautions to mitigate damages by preventing future fraud.

74. Defendants' breaches of duty caused Plaintiff and Class members to suffer from identity theft, loss of time and money to monitor their finances for fraud, and loss of control over their Private Information.

75. As a result of Defendants' negligence and breach of duties, Plaintiff and Class members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

76. Plaintiff seeks the award of actual damages on behalf of Plaintiff and on behalf of the Class members.

77. In failing to secure Plaintiff and Class members' Private Information and promptly notifying them of the Data Breach, Defendants are guilty of oppression, fraud, intentional misconduct, gross negligence, malice, or deceit, in that Defendants acted or failed to act with a willful and conscious disregard of Plaintiff and Class members' rights.

78. Plaintiff seeks injunctive relief on behalf of the Classes in the form of an order (1) compelling Defendants to institute appropriate data collection and safeguarding methods and policies with regard to patient information; and (2) compelling Defendants

to provide detailed and specific disclosure of what types of Private Information have been compromised as a result of the data breach.

SECOND COUNT
Breach of Express Contract
(On Behalf of Plaintiff and the Nationwide and Georgia Classes)

79. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

80. Plaintiff and Class members, upon information and belief, entered into express contracts with Defendants that include Defendants' promise to protect nonpublic personal information given to Defendants or that Defendants gather on their own from disclosure.

81. Plaintiff and Class members performed their obligations under the contract when they engaged and used the AIMSweb platform.

82. Defendants breached their contractual obligation to protect the nonpublic personal information Defendants gathered when the information was accessed by unauthorized personnel as part of the Data Breach.

83. As a direct and proximate result of the breach, Plaintiff and Class members have been harmed and have suffered, and will continue to suffer, damages and injuries.

THIRD COUNT
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide and Georgia Classes)

84. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

85. Defendants provided Plaintiff and Class members with an implied contract to protect and keep private the Plaintiff and Class members' PII when they gathered such information as each Plaintiff and Class members engaged and used the AIMSweb platform.

86. Plaintiff and Class members would not have provided their PII to Defendants, but for Defendants' implied promises to safeguard and protect Plaintiff's and Class members' PII.

87. Plaintiff and Class members performed their obligations under the implied contract when they provided their PII and when they engaged in using the AIMSweb platform provided by Defendants.

88. Defendants breached the implied contracts with Plaintiff and Class members by failing to protect and keep private Plaintiff and Class members' PII.

89. As a direct and proximate result of Defendants' breach of their implied contracts, Plaintiff and Class members have been harmed and have suffered, and will continue to suffer, damages and injuries.

FOURTH COUNT
Intrusion Upon Seclusion / Invasion of Privacy
(On Behalf of Plaintiff and the Multi-State Class)

90. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

91. Plaintiff and Class members had a reasonable expectation of privacy in the PII Defendants mishandled.

92. Defendants' conduct as alleged above intruded upon Plaintiff and the Class members' seclusion under common law.

93. By intentionally failing to keep Plaintiff and Class members' PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendants intentionally invaded Plaintiff and Class members' privacy by:

a. Intentionally and substantially intruding into Plaintiff and Class members' private affairs in a manner that identifies the Plaintiff and Class members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiff and Class members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to the Plaintiff and Class members.

94. Defendants knew that an ordinary person in Plaintiff or Class members' position would consider Defendants' intentional actions highly offensive and objectionable.

95. Defendants invaded Plaintiff and Class members' right to privacy and intruded into Plaintiff and Class members' private affairs by intentionally misusing and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

96. Defendants intentionally concealed from Plaintiff and Class members an incident that misused and/or disclosed their PII without their informed, voluntary, affirmative, and clear consent.

97. As a proximate result of such intentional misuse and disclosures, Plaintiff and Class members' reasonable expectations of privacy in their PII were unduly frustrated and thwarted. Defendants' conduct amounted to a substantial and serious invasion of Plaintiff and Class members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendants' intentional actions or inaction highly offensive and objectionable.

98. In failing to protect Plaintiff and Class members' PII, and in intentionally misusing and/or disclosing their PII, Defendants have acted with intentional malice and oppression and in conscious disregard of Plaintiff and Class members' rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages on behalf of herself and the Class.

FIFTH COUNT
Violation of the Georgia Fair Business Practices Act
(On Behalf of Plaintiff and the Georgia Subclass)

99. Plaintiff repeats and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

100. The Georgia Fair Business Practices Act ("FBPA"), OCGA §§ 10-1-390 *et seq*., prohibits the use of unfair or deceptive business practices in the conduct of trade or commerce. The FBPA is to be liberally construed to effectuate its purposes. OCGA § 10-1-391.

101. Defendants' unfair or deceptive business practices include, but are not limited to, the following:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Georgia Subclass members' PII, which was a direct and proximate cause of the Data Breach;

b. Misrepresenting in their Privacy Notice that consumers should "expect information to be treated with total confidentiality," that Pearson takes "full responsibility for the information [they] hold about you" and acknowledges an awareness of and the obligation to "comply with all relevant data protection laws";

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Georgia Subclass Members PII, including duties imposed by the Federal Trade Commission Act, 15 U.S.C. § 45; and

d. Omitting or concealing the material fact that they did not reasonably or adequately safeguard Plaintiff and Georgia Subclass Members' PII.

102. It is alleged on information and belief that Defendants' violations of the FBPA set forth herein were done with awareness of the fact that the conduct alleged was wrongful and were motivated solely for increased profit. It is also alleged on information and belief that Defendants did these acts knowing the harm that would result to Plaintiff

and the Georgia Subclass members and that Defendants did these acts notwithstanding that knowledge.

103. Plaintiff and Georgia Subclass members suffered an "injury in fact" as a result of Defendants' actions alleged herein.

104. As a result, Plaintiff and Georgia Subclass members seeks all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiff and her Counsel to represent the Classes;

b) For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff and Class members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

c) For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

e) Ordering Defendants to pay for not less than three years of credit monitoring services for Plaintiff and the Classes;

f) Ordering Defendants to disseminate individualized notice of the Data Breach to all Class members;

g) For an award of actual damages and compensatory damages, in an amount to be determined, as allowable by law;

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

i) Pre- and post-judgment interest on any amounts awarded; and

j) Such other and further relief as this court may deem just and proper.

Dated: October 30, 2019

Respectfully submitted,

/s/ *Melissa S. Weiner*

PEARSON, SIMON & WARSHAW, LLP
Melissa S. Weiner (#0387900)
Joseph C. Bourne (#0389922)
800 LaSalle Avenue, Suite 2150
Minneapolis, Minnesota 55402
Telephone: (612) 389-0600
Facsimile: (612) 389-0610
mweiner@pswlaw.com
jbourne@pswlaw.com

WHITFIELD BRYSON & MASON LLP
Gary E. Mason (*pro hac vice forthcoming*)
5101 Wisconsin Ave., NW, Ste. 305
Washington, DC 20016
Telephone: 202.640.1160
Facsimile: 202.429.2294
gmason@wbmllp.com

KOZONIS & KLINGER, LTD.
Gary M. Klinger (*pro hac vice forthcoming*)
4849 N. Milwaukee Ave., Ste. 300
Chicago, Illinois 60630
Telephone: 312.283.3814
Facsimile: 773.496.8617
gklinger@kozonislaw.com

Attorneys for Plaintiff and the Proposed Classes