IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF VIRGINIA
Abingdon Division

Kyle Beer, individually and on behalf of all others similarly situated, Plaintiff, v. Bluefield University, Defendant.	Case No. 1:23CV00055 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Kyle Beer ("Plaintiff"), individually and on behalf of all other similarly situated individuals (the "Class Members," as defined below), by and through his counsel, files this Class Action Complaint against Bluefield University ("Bluefield" or "Defendant") and alleges the following based on personal knowledge of facts pertaining to himself and on information and belief based on the investigation of counsel as to all other matters.

INTRODUCTION

1. Defendant is private Baptist university in Bluefield, Virginia, offering 22 majors to students from 32 different states and 16 countries.[1]

2. Defendant obtains, collects, uses, and derives a benefit from the Personal Identifying Information ("PII") of Plaintiff and Class Members. As such, Defendant assumed the legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

[1] https://www.bluefield.edu/about-bluefield-university/quick-facts/

3. This class action seeks to redress Defendant's unlawful, willful and wanton failure to reasonably protect the sensitive PII of the Plaintiff and Class Members (as defined below), in violation of Defendant's legal obligations. Defendant failed to properly safeguard and protect the PII in its possession, thereby allowing cybercriminals the opportunity to steal Plaintiff's and Class Members' valuable PII from Defendant's inadequate cybersecurity.

4. On May 1, 2023, Defendant became aware of unauthorized access to its network that resulted in the exposure of data maintained on its network (the "Data Breach").

5. Plaintiff's and Class Members' PII was compromised due to Defendant's negligent and/or careless acts and omissions and their failure to protect the PII of Plaintiff and Class Members.

6. At this time, there exist many Class Members who are totally unaware their PII has been compromised, and that they are at significant risk of identity theft and various other forms of personal, social, and financial harm. Defendant admits that at least 23,195 individual's PII has been compromised in the Data Breach.

7. Plaintiff brings this action, individually, and on behalf of all others whose PII was compromised as a result of Defendant's failure to adequately protect PII, timely discover the breach, and warn its applicants, students, and employees of its inadequate information security practices, and effectively monitor its platforms for security vulnerabilities and incidents.

8. Plaintiff and Class Members have all suffered injury as a result of the Defendant's negligent conduct, including: (i) the potential for Plaintiff's and Class Members' exposed PII to be sold and distributed on the dark web, (ii) a lifetime risk of identity theft, sharing, and detrimental use of their sensitive information, (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII, (iv) lost

opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and (v) the continued and increased risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to take appropriate and adequate measures to protect its applicants', students', and employees' PII.

9. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to equitable and injunctive relief.

I. THE PARTIES

10. Plaintiff Kyle Beer is an individual domiciled in and is a citizen of Woodbridge, Virginia, which is located in Prince William County. On or about November 27, 2023, Defendant sent Plaintiff Beer a letter informing him he had been a victim of the Data Breach.

11. Defendant Bluefield University is a Virginia private university located in Bluefield, Virginia, which is located in Tazewell County.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act (CAFA) and 28 U.S.C. § 1332(d) because this is a class action involving more than 100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and many members of the class are citizens of states different from Defendant.

13. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, and it regularly transacts business in this District.

14. Venue is proper in this district pursuant to 28 U.S.C. §1391(b)(2) because the Western District of Virginia is a judicial district in which a substantial part of the events giving rise to the claim occurred.

II. FACTUAL ALLEGATIONS

A. Defendant and Its Collection of PII

15. Defendant is a private university located in Bluefield, Virginia.

16. As a condition to applying to Bluefield. enrolling as a student, and being employed, Defendant collects the PII of the Plaintiff and Class Members.

17. In order to apply to or enroll in Bluefield University, Plaintiff and Class Members were required to and did in fact turn over PII to Defendant.

18. For example, according to the Bluefield's Privacy Policy, Defendant admits to collecting individuals' PII and using personal data for "legitimate business".[2]

19. In the Privacy Policy, Defendant falsely warrants that "The University implements reasonable physical, technical, and administrative safeguards designed to prevent the unauthorized access to or use of the information [Defendant] collects online."[3]

20. Despite their promises to safeguard Plaintiff and Class Members' PII, Defendant failed to implement and adopt reasonable measures to protect against involuntary disclosures to unauthorized third parties.

21. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to unauthorized third parties.

B. The Data Breach

22. On May 1, 2023, Defendant allowed an unknown hacker to gain access to and steal the Plaintiff's and the Class Members' PII.

23. On or around November 27, 2023, Defendant publicly disclosed that, "Bluefield

[2] https://www.bluefield.edu/bu-privacy-notice/

[3] *Id*.

detected unauthorized access to [its] network as a result of a cybersecurity incident that resulted in the potential exposure of data [Defendant] maintain[s]."[4]

24. Upon information and belief, the personal information stolen in the Data Breach includes PII, such as: names, Social Security numbers, student ID numbers, and student records.[5]

25. Defendant knew of its duties to Plaintiff and the Class Members, and the risks associated with failing to protect the PII entrusted to it. Defendant knew that if it did not use adequate data security capabilities that Plaintiff's and the Class's PII would be unlawfully exposed.

26. Further, Defendant had notice of the Data Breach as early as May 1, 2023. Yet, Defendant negligently delayed in responding to the breach and informing Plaintiff and the Class of the breach.

27. On or around November, 27 2023, Defendant began sending Plaintiff and Class Members a notice of the Data Breach ("Notice of the Data Breach").[6]

28. Defendant admitted in the Notice of the Data Breach that an unauthorized actor accessed and "removed" sensitive personal information about Plaintiff and Class Members.

29. The details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

30. The unencrypted PII of Plaintiff and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted

---

[4] *See* **Exhibit 1**

[5] *Id*.

[6] *Id*.

marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

31. Defendant was negligent and did not use or implement reasonable security procedures, oversight and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing the exposure and theft of PII for Plaintiff and Class Members.

32. Because Defendant had a duty to protect Plaintiff's and Class Members' PII, Defendant should have known through readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

33. In May of 2023, Higher Ed Dive published online an article titled, "Ransomware threat against colleges grows, survey finds" that, among other things, warned that "ransomware attacks targeted the education sector more than any other industry in the last year, with 79% of surveyed higher education institutions across the world reporting being hit…."[7] Further, in July of 2022, Inside Higher Ed published an online article titled, "Ransomware Attacks Against Higher Ed Increase", which stated, "[c]olleges and universities worldwide experienced a surge in ransomware attacks in 2021, and those attacks had significant operational and financial costs, according to a new report from Sophos, a global cybersecurity leader."[8]

---

[7] Higher Ed Dive, Ransomware threat against colleges grows, survey finds (May 10, 2023) (emphasis added), available at https://www.highereddive.com/news/ransomware-threat-colleges-grows-sophos/649976/#:~:text=Sophos'%20latest%20survey%20suggests%20that,incidents%20in%20the%20latest%20survey (last visited December 7, 2023).

[8] Inside Higher Ed, Ransomware Attacks Against Higher Ed Increase (July 21, 2022) (emphasis added), available at https://www.insidehighered.com/news/2022/07/22/ransomware-attacks-against-higher-ed-increase (last visited December 7, 2023).

34. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."[9]

35. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[10]

36. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that: (i) cybercriminals were targeting the education sector, such as Defendant, (ii) cybercriminals were ferociously aggressive in their pursuit of organizations and universities in possession of significant sensitive information such as Defendant, (iii) cybercriminals were leaking sensitive information on dark web portals, and (iv) cybercriminals' tactics included threatening to release stolen data.

37. Considering the information readily available and accessible on the internet before the Data Breach and Defendant's involvement in data breach litigation, Defendant, having elected to store the unencrypted PII of Plaintiff and Class Members, had reason to know that Plaintiff's

---

[9] 5 ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), available at https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited December 7, 2023).

[10] U.S. CISA, Ransomware Guide – September 2020, available at https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf (last visited December 7, 2023).

and the Class Members' PII was at risk for being shared with unknown and unauthorized persons.

38. Prior to the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiff's and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack.

39. Prior to the Data Breach, Defendant knew or should have known that it should have confirmed the information it obtained was encrypted within the PII to protect against their publication and misuse in the event of a cyberattack.

40. Since the breach, Defendant continues to store applicant, student, and employee information, including Plaintiff's and Class Members' PII, and has failed to give adequate assurances that it has enhanced its security practices sufficiently to avoid another breach.

C. Plaintiff's Experiences

Plaintiff Kyle Beer

41. Upon information and belief, Plaintiff Beer applied to Bluefield University in November of 2021 and received Defendant's Notice of the Data Breach on or around November 27, 2023.

42. Defendant acquired, collected, and stored Plaintiff's PII.

43. Defendant was obligated by law, regulations, and guidelines to protect Plaintiff's and the Class's PII and to ensure it maintained adequate data security for Plaintiff's and the Class's PII.

44. Defendant was in possession of Plaintiff's PII before, during, and after the Data Breach.

45. Plaintiff received Defendant's Notice of Data Breach on November 27, 2023. The Notice stated that the PII accessed and acquired in the Data Breach included Plaintiff's name, Social Security number, student ID number, and student records.

46. As a result of the Data Breach, Plaintiff's sensitive information was accessed and stolen by an unauthorized actor, including his name, Social Security number, student ID number, and student records. Defendant has not yet provided definitive findings for Plaintiff to know. The confidentiality of Plaintiff's sensitive information has been irreparably harmed. For the rest of his life, Plaintiff will have to worry about when and how his sensitive information may be shared or used to his detriment.

47. As a result of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, researching credit monitoring and/or identity theft protection services, enrolling in credit monitoring and/or identity theft protection services, reviewing credit reports, reviewing account statements, and mitigating fraud/identity theft. This time has been lost forever and cannot be recaptured.

48. Additionally, Plaintiff is very careful about sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

49. Plaintiff stores any documents containing his sensitive PII in safe and secure locations or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

50. As a direct and traceable result of the Data Breach, Plaintiff suffered actual damages such as: (i) lost time related to monitoring his accounts for fraudulent activity; (ii) loss of privacy due to his PII being exposed to cybercriminals; (iii) loss of the benefit of the bargain

because Defendant did not adequately protect his PII; (iv) severe emotional distress because identity thieves now possess his PII; (v) exposure to increased and imminent risk of fraud and identity theft now that his PII has been exposed; (vi) the loss in value of his PII due to his PII being in the hands of cybercriminals who can use it at their leisure; (vii) actual misuse of his PII; and (viii) other economic and non-economic harm.

51. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from the Data Breach.

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

53. To his knowledge, Plaintiff has not been the victim of any other data breach.

D. Cyber Criminals Will Use Plaintiff's PII to Further Defraud Him

54. PII is of great value to hackers and cyber criminals, and the data stolen in the Data Breach can and will be used in a variety of ways by criminals to exploit Plaintiff and the Class Members to profit off their misfortune.

55. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[11] For example, with the PII stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims'

[11] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity") (last accessed December 7, 2023).

names to police during arrests, and many other harmful forms of identity theft.[12] These criminal activities have and will result in devastating financial and personal losses to Plaintiff Beer and the Class Members.

56. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[13]
>
> [Emphasis added.]

57. This was a financially motivated and targeted Data Breach, as the only reason the cyber criminals go through the trouble of running a targeted cyberattack is to get information that they can monetize by selling it on the black market for use in the kinds of criminal activity described herein. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[14] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[15]

---

[12] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 15, 2017, https://www.usatoday.com/story/money/personalfinance/2017/11/15/5-ways-identity-thief-can-use-your-social-security-number/860643001/

[13] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[14] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, Nov. 15, 2017, https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web

[15] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

58. Hackers may not use the information right away, but this does not mean it will not be used. 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.[16]

59. For instance, with a stolen social security number, which is part of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[17]

60. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.

61. Defendant's offer of one year of Cyberscout through Identity Force to Plaintiff and the Class is woefully inadequate and will not fully protect them from the damages and harm caused by Defendant's data security failures. While some harm has begun already, the full scope of the harm has yet to be realized. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. Once the twelve-months have expired, Plaintiff and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to Defendant's gross negligence. Furthermore, identity monitoring only alerts someone to the fact that they have *already been the victim of identity*

---

[16] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,* GAO, June 4, 2007, https://www.gao.gov/assets/gao-07-737.pdf

[17] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 15, 2017, https://www.usatoday.com/story/money/personalfinance/2017/11/15/5-ways-identity-thief-can-use-your-social-security-number/860643001/

theft (*i.e.*, fraudulent acquisition and use of another person's PII)—it does not prevent identity theft.[18] Nor can an identity monitoring service remove personal information from the dark web.[19] "The people who trade in stolen personal information [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."[20]

62. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from continued fraud and identity theft. Plaintiff and Class Members must now take the time and effort to mitigate the actual and potential impact of the Data Breach in their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come. Even more seriously is the identity restoration that Plaintiff and other Class Members must go through, which can include spending countless hours filing police reports, filling out IRS forms, Federal Trade Commission checklists, Department of Motor Vehicle driver's license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiff and Class Members must take.

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

[19] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America, Mar. 19, 2019, https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[20] *Id.*

63. Plaintiff and Class Members have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Trespass, damage to, and theft of their personal property including PII;

b. Improper disclosure of their PII;

c. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals;

d. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their PII and that identity thieves may use that information to defraud other victims of the Data Breach;

e. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach; and

f. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class Members' personal information for which there is a well-established and quantifiable national and international market.

64. Moreover, Plaintiff and Class Members have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard security measures and safeguards. Defendant has shown themselves wholly incapable of protecting Plaintiff's and Class Members' PII.

65. Defendant themselves acknowledged the harm caused by the Data Breach because it offered Plaintiff and Class Members the woefully inadequate twelve months of single bureau credit monitoring, credit report, and credit score services, and twelve months of Cyberscout

through Identity Force. Twelve months of credit monitoring and fraud services is, however, inadequate to protect Plaintiff and Class Members from a lifetime of identity theft risk.[21]

66. Defendant further acknowledged, in its letter to Plaintiff and other Class Members, that Bluefield needed to improve its security protocols, stating: "[w]e continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information."[22]

67. The Breach Notice further acknowledged that the Data Breach would cause inconvenience to affected individuals and that financial harm would likely occur, stating: "you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis."

68. At Defendant's suggestion, Plaintiff and Class Members are desperately trying to mitigate the damage that Defendant's Data Breach has caused them. Given the kind of PII Defendant allowed to be stolen, Plaintiff and Class Members are certain to incur additional damages. Because identity thieves have their PII and are already using it, Plaintiff and Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[23]

69. None of this should have happened.

---

[21] *See* **Exhibit 1**.

[22] *Id.*

[23] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

E. Defendant Was Aware of the Risk of Cyber Attacks

70. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the names of some of the biggest cybersecurity breaches: Target,[24] Yahoo,[25] Marriott International,[26] Chipotle, Chili's, Arby's,[27] and others.[28]

71. Defendant, who requires the collection and maintenance of highly sensitive and valuable PII, should certainly have been aware, and indeed was aware, that not encrypting PII created a substantial risk for a data breach that could expose the PII it collected and maintained.

72. With the increasing prevalence of data breach announcements, Defendant certainly recognized it had a duty to use reasonable measures to protect the wealth of PII that it collected and maintained.

---

[24] Michael Kassner, *Anatomy of the Target Data Breach: Missed Opportunities and Lessons Learned*, ZDNET (Feb. 2, 2015), https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/.

[25] Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSOONLINE.COM (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html.

[26] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/.

[27] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[28] *See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

73. In 2022, a total of 1,802 data breaches occurred, which represents the second highest number of data events in a single year and just 60 events short of the all-time record of 1,862 in 2021. The education sector had 65 compromises affecting 888,905 individuals.[29]

74. In light of the significant number of data breaches that occurred in the education sector in 2022, Defendant knew or should have known that Plaintiffs' and Class Members' PII would be targeted by cybercriminals.

75. Defendant was clearly aware of the risks it was taking when failing to ensure it had adequate data security.

F. Defendant Could Have Prevented the Breach

76. Data breaches are preventable.[30] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[31] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[32]

77. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information

[29] ITRC_2022-Data-Breach-Report_Final-1.pdf (idtheftcenter.org)

[30] Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[31] *Id.* at 17.

[32] *Id.* at 28.

security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[33]

78. In a Data Breach like this, many failures laid the groundwork for the Breach. The FTC has published guidelines that establish reasonable data security practices for businesses. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[34] The guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommended that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

79. Upon information and belief, Defendant failed to comply with the reasonable and necessary industry standards necessary to prevent a data breach, including the FTC's guidelines. Upon information and belief, Defendant also failed to ensure that the Defendant met the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program

---

[33] *Id.*

[34] FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

(FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in reasonable cybersecurity preparation.

80. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[35]

81. To prevent and detect cyber-attacks, including the attack that resulted in the Data Breach, Defendant could and should have ensured it implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

[35] *See* How to Protect Your Networks from RANSOMWARE, at 3, *available at* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[36]

82. Further, to prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)….

[36] *Id.* at 3-4.

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it….

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic….[37]

83. In addition, to prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Secure internet-facing assets**

  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audit; remove privileged credentials

- **Thoroughly investigate and remediate alerts**

  - Prioritize and treat commodity malware infections as potential full compromise;

- **Include IT Pros in security discussions**

[37] *See* Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* https://www.cisa.gov/news-events/news/protecting-against-ransomware

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

- **Build credential hygiene**

  - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

- **Apply principle of least-privilege**

  - Monitor for adversarial activities
  - Hunt for brute force attempts
  - Monitor for cleanup of Event Logs
  - Analyze logon events

- **Harden infrastructure**

  - Use Windows Defender Firewall
  - Enable tamper protection
  - Enable cloud-delivered protection
  - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].[38]

84. Given that Defendant stored the PII of thousands of individuals, including the PII of Plaintiff and the Class Members, Defendant could and should have ensured the Bluefield systems were capable of preventing and detecting cyber-security attacks.

85. Defendant acquired, collected, and stored the PII of Plaintiff and Class Members.

86. Plaintiff and other Members of the Class entrusted their PII to Defendant.

87. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

88. Given that Defendant was storing the PII of other individuals, Defendant could and

[38] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

should have implemented all of the above measures to prevent and detect cyber-security attacks.

89. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of Plaintiff and Class Members.

90. Defendant could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing the PII of Plaintiff and Class Members and ensuring Defendant properly secured and encrypted the folders, files, and/or data fields containing the PII of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data it no longer had a reasonable need to maintain or only stored data in an Internet accessible environment when there was a reasonable need to do so.

91. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

92. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

G. Defendant's Response to the Data Breach is Inadequate to Protect Plaintiff and the Class

93. Defendant failed to inform Plaintiff and Class Members of the Data Breach in time for them to protect themselves from identity theft.

94. Defendant stated that "[o]n May 1, 2023, Bluefield detected unauthorized access to our network as a result of a cybersecurity incident that resulted in the potential exposure of the

data we maintain."[39] Further, Defendant stated, "Bluefield discovered on October 26, 2023, that your personal information was potentially removed from our network by the unauthorized party."[40] Despite learning of the Data Breach on May 1, 2023, Defendant did not begin notifying the Plaintiff and Class Members until November 27, 2023—almost six (6) after knowledge of the breach.

95. During these intervals, the cybercriminals had the opportunity to exploit the Plaintiff and Class Members' PII while Defendant was sitting idle and secretly still investigating the Data Breach.

H. Defendant Failed to Comply with FTC Guidelines

96. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which 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.

97. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[41] The guidelines also recommend businesses use an intrusion detection system to expose a breach as soon

[39] *See* **Exhibit 1**

[40] *Id*.

[41] https://www.bulkorder.ftc.gov/system/files/publications/2_9-00006_716a_protectingpersinfo-508.pdf

as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

98. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient 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 Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

99. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

100. Defendant was always fully aware of their obligations to protect the PII of Plaintiff and Class Members and the significant repercussions that would result from its failure to ensure it utilized adequate cybersecurity measures.

III. CLASS ACTION ALLEGATIONS

101. Plaintiff incorporates by reference all preceding paragraphs as if fully restated here.

102. Plaintiff brings this action against Defendant on behalf of themselves and all other individuals similarly situated under Federal Rule of Civil Procedure 23. Plaintiff asserts all claims on behalf of a nationwide class (the "Class") defined as follows:

> All natural persons residing in the United States whose personal identifiable information (PII) was compromised as a result of the Data Breach announced by Defendant on or about November 27, 2023.

103. Excluded from the Class is the Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

104. Plaintiff reserves the right to amend the above definition or to propose subclasses in subsequent pleadings and motions for class certification.

105. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

106. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. According to the Attorney General for the State of Maine Data Breach Notifications, the total number of persons affected by the Data Breach is 23,195.

107. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Defendant's uniform misconduct. All had their PII compromised as a result of the Data Breach.

108. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and their counsel.

109. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the

Class individually to effectively redress Defendant's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

110. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

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

b. Whether Defendant failed to adequately safeguard Plaintiff's and Class Members' PII;

c. Whether Defendant owed a duty to Plaintiff and the Class to ensure its systems were capable of adequately protecting their PII, and whether it breached this duty;

d. Whether Defendant breached its duties to Plaintiff and the Class as a result of the Data Breach;

e. Whether Defendant failed to ensure its systems provided adequate cyber security;

f. Whether Defendant knew or should have known its systems and software were vulnerable to cyber-attacks;

g. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its company network;

h. Whether Defendant was negligent in failing to ensure its systems and software adhered to reasonable retention policies, thereby greatly increasing the size of the Data Breach;

i. Whether Defendant breached implied contractual duties to Plaintiff and Class Members to use reasonable care in protecting their PII;

j. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and Class Members;

k. Whether Defendant continues to breach duties to Plaintiff and Class Members;

l. Whether Plaintiff and the Class suffered injury as a proximate result of Defendant's negligent actions or failures to act;

m. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief; and

n. Whether Defendant's actions alleged herein constitute gross negligence, and whether Plaintiff and Class Members are entitled to punitive damages.

IV. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

111. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

112. While receiving the PII of applicants, students, and employees, Bluefield gathered and stored the PII of Plaintiff and Class Members.

113. Defendant had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed. Defendant had a duty to Plaintiff and each Class Member to exercise reasonable care in holding, safeguarding, and protecting that information. Plaintiff and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class Members had no ability to protect their PII that was in Defendant's possession. As such, a special relationship existed between the Defendant and the Plaintiff and Class Members.

114. Defendant was well aware of the fact that cyber criminals routinely target higher education facilitators, including universities, through cyberattacks in an attempt to steal the PII of employees, applicants, students, and business associates.

115. Defendant owed Plaintiff and Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data and provide notification to Plaintiff and Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

116. Defendant had duties to protect and safeguard the PII of Plaintiff and Class Members from potential cyberattacks, including by ensuring its systems and software: (i) encrypted any document or report containing PII, (ii) did not permit documents containing unencrypted PII to be maintained on its systems, and (iii) took other similarly common-sense precautions when dealing with sensitive PII. Additional duties that Defendant owed Plaintiff and Class Members include:

a. Exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in its possession;

b. Protect the PII in its possession using reasonable and adequate security procedures and systems;

c. Ensure its systems and software were adequately and properly audited and tested;

d. Ensure its systems and software did not store PII for longer than absolutely necessary;

e. Implement processes to quickly detect a data breach, security incident, or intrusion; and

f. Promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

117. Plaintiff and Class Members were the intended beneficiaries of Defendant's duties, creating a special relationship between them. Defendant was in a position to ensure that its systems and software were sufficient to protect the PII that Plaintiff and the Class had entrusted to it Defendant.

118. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class Members' PII. Defendant breached its duties by, among other things:

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

b. Failing to ensure its systems and software were capable of protecting the PII in its possession using reasonable and adequate security procedures and systems;

c. Failing to ensure its systems and software were adequately and properly audited and tested to avoid cyberattacks;

d. Failing to train its employees regarding how to properly and securely transmit and store PII, including maintaining PII in an encrypted format;

e. Failing to consistently enforce security policies aimed at protecting Plaintiff and Class Members' PII;

f. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions;

g. Failing to abide by reasonable retention and destruction policies for PII of former applicants, students, and employees; and

h. Failing to promptly and accurately notify Plaintiff and Class Members of the Data Breach that affected their PII.

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

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

121. The damages Plaintiff and Class Members have suffered (as alleged above) were and are reasonably foreseeable.

122. The damages Plaintiff and the Class have and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

123. Plaintiff and the Class have suffered injury and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

124. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

125. Plaintiff's and Class Members' PII was provided to Defendant as a condition of applying to Bluefield, attending Bluefield, or being employed by Bluefield.

126. When Plaintiff and Class Members provided their PII to Defendant as a condition to applying or attending Bluefield, they entered into implied contracts through Defendant's conduct in which Defendant agreed to comply with its statutory and common law duties to protect their PII and to timely notify them in the event of a Data Breach.

127. When Plaintiff and Class Members provided their PII to Defendant as part of their receipt of services, they entered into implied contracts in which Defendant agreed to comply with its duties promised in its Privacy Policy, including the promise to implement "reasonable physical, technical, and administrative safeguards designed to protect unauthorized access to or use of information [Defendant] collects online".

128. Based on Defendant's legal obligations and promises, Defendant had an implied duty to safeguard their PII through the use of reasonable industry standards.

129. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class Members' PII and failing to provide them with timely and accurate notice of the Data Breach. Indeed, it took Defendant almost six (6) months to begin warning Plaintiff and Class Members of their imminent risk of identity theft.

130. As a direct and proximate result of Defendant's breach of implied contract, Plaintiff and the Class Members have suffered damages, including foreseeable consequential damages that Defendant knew about when it requested Plaintiff's and the Class Members' PII.

131. Plaintiff and the Class have suffered injury, and are entitled to actual and punitive damages, statutory damages, and reasonable attorneys' fees and costs, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

132. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

133. Pursuant to the FTC Act, 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 the Class's PII.

134. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Class's PII.

135. Defendant breached its respective duties to Plaintiff and Class Members under the FTC Act by inadequately protecting its systems and software and failing to ensure its systems and software provided fair, reasonable, or adequate data security to safeguard PII.

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

137. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant collected and stored and the

foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

138. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against organizations that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

139. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

140. The injuries and harm suffered by Plaintiff and members of the Class was the reasonably foreseeable result of Defendant's breach of duties. Defendant knew or should have known its systems and software were incapable of safeguarding Plaintiff's and Class Members' PII and that a breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

141. Had Plaintiff and the Class known that Defendant did not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

142. Defendant's various violations and failure to comply with applicable laws and regulations constitutes negligence per se.

143. As a direct and proximate result of Defendant's negligence per se, Plaintiff and the Class have suffered harm, including actual misuse of their PII; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

144. Additionally, as a direct and proximate result of Defendant's negligence per se, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant's fails to undertake appropriate and adequate measures to protect their PII in their continued possession.

FOURTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

145. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

146. A relationship existed between Plaintiff and the Class Members and Defendant in which Plaintiff and the Class put their trust in Defendant to protect their PII. Defendant accepted this duty and obligation when it received Plaintiff and the Class Members' PII.

147. Plaintiff and the Class Members entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for educational, research, marketing, or other purposes related to Bluefield.

148. Plaintiff and the Class Members were required to provide their PII to Defendant in exchange to applying, attending, or being employed by Defendant, and Plaintiff and Class Members placed special confidence in Defendant by entrusting it with their PII.

149. Defendant knew or should have known that the failure to exercise due care in the collecting, storing, and using of individual's PII involved an unreasonable risk of harm to Plaintiff and the Class, including harm that foreseeably could occur through the criminal actions of a third party.

150. Defendant's fiduciary duty required it to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or

disclosed to unauthorized parties. This duty includes, among other things, ensuring and monitoring Defendant's system and software's design, maintenance, and testing of its security protocols to ensure that Plaintiff and the Class's information was adequately secured and protected.

151. Defendant also had a fiduciary duty to ensure that its systems and software had procedures in place to detect and prevent improper access and misuse of Plaintiff's and the Class's PII. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Defendant was entrusted with Plaintiff and the Class's PII.

152. Defendant breached its fiduciary duty that it owed Plaintiff and the Class by failing to act in good faith, fairness, and honesty; by failing to act with the highest and finest loyalty; and by failing to protect the PII of Plaintiff and the Class Members.

153. Defendant's breach of fiduciary duties was a legal cause of damages to Plaintiff and the Class.

154. But for Defendant's breach of fiduciary duty, the damage to Plaintiff and the Class would not have occurred, and the Data Breach contributed substantially to producing the damage to Plaintiff and the Class.

155. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff and the Class are entitled to actual, consequential, and nominal damages and injunctive relief, with amounts to be determined at trial.

FIFTH CAUSE OF ACTION
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

156. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

157. Plaintiff and Class Members have a reasonable expectation of privacy in their PII.

158. Defendant's negligent, reckless, and intentional conduct as alleged herein invaded Plaintiff's and Class Members' privacy.

159. By knowingly failing to keep Plaintiff's and Class Members' PII safe, and by knowingly misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendant intentionally invaded Plaintiff's and Class Members' privacy by intruding into Plaintiff's and Class Members' private affairs, without approval, in a manner that identifies Plaintiff and Class Members and that would be highly offensive and objectionable to a person of ordinary sensibilities.

160. Defendant knew that an ordinary person in Plaintiff's or a Class Member's position would consider Defendant's intentional actions highly offensive and objectionable.

161. Such an intentional intrusion into Plaintiff's and Class Members' private affairs is likely to cause outrage, shame, and mental suffering because of the PII disclosed.

162. Defendant invaded Plaintiff's and Class Members' right to privacy and intruded into Plaintiff's and Class Members' private life by negligently, recklessly, and intentionally misusing and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

163. The PII disclosed by Defendant has no legitimate reason to be known by the public.

164. Defendant intentionally concealed from Plaintiff and Class Members an incident that misused and/or disclosed their PII without their informed, voluntary, affirmative, and clear consent.

165. As a proximate result of such intentional misuse and disclosures, Plaintiff's and Class Members' reasonable expectations of privacy in their PII was unduly frustrated and

thwarted. Defendant's conduct, amounting to a substantial and serious invasion of Plaintiff's and Class Members' protected privacy interests causing anguish and suffering such that a person with ordinary sensibilities would consider Defendant's intentional actions or inaction highly offensive and objectionable.

166. In failing to protect Plaintiff's and Class Members' PII, and in negligently, recklessly, and intentionally misusing and/or disclosing their PII, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private. Plaintiff, therefore, seeks an award of damages on behalf of himself and the Class.

SIXTH CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

167. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here. This Count is pled in the alternative to the Breach of Implied Contract Count above.

168. Plaintiff and Class Members conferred a monetary benefit on Defendant by providing Defendant with their valuable PII.

169. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

170. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

171. Under the 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 appropriate data management and security measures that are mandated by industry standards.

172. Defendant acquired the monetary benefit and PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

173. If Plaintiff and Class Members knew that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

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

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

176. Defendant should be compelled to disgorge into a common fund or constructive

trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them.

SEVENTH CAUSE OF ACTION
Injunctive and Declaratory Relief
(On Behalf of Plaintiff and the Class)

177. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged here.

178. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

179. As previously alleged and pleaded, Defendant owes duties of care to Plaintiff and Class Members that require them to adequately secure their PII.

180. Defendant still possesses the PII of Plaintiff and the Class Members.

181. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class Members.

182. Defendant has claimed that it will "continually evaluate and modify our practices and internal controls to enhance the security and privacy of [Plaintiff's and Class Members'] personal information." But there is nothing to prevent Defendant from reversing any changes made once it has weathered the increased public attention resulting from this Breach.

183. Plaintiff, therefore, seeks a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering Defendant to engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated

attacks, penetration tests, and audits on its systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering Defendant to significantly increase its spending on cybersecurity including systems and personnel;

c. Ordering Defendant to engage third-party security auditors and internal personnel to run automated security monitoring;

d. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;

e. Ordering that Defendant protect Plaintiff's and the Class's PII by, among other things, guaranteeing it has firewalls and access controls so that if one area of Defendant's systems are compromised, hackers cannot gain access to other portions of its systems;

f. Ordering that Defendant cease storing unencrypted PII on its systems;

g. Ordering that Defendant conduct regular database scanning and securing checks;

h. Ordering Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

i. Ordering Defendant to implement and enforce adequate retention policies for PII, including destroying, in a reasonably secure manner, PII once it is no longer necessary for it to be retained; and

j. Ordering Defendant to meaningfully educate its current, former, and

prospective employees and subcontractors about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves.

V. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including compensatory damages, punitive damages, attorneys' fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

VI. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Class Action Complaint

Dated: December 9, 2023

Respectfully submitted,

Craig Marchiando, VSB #89736
CONSUMER LITIGATION ASSOCIATES, P.C.
763 J. Clyde Morris Blvd., Suite 1-A
Newport News, VA 23601
(757) 930-3660 – Telephone
(757) 930-3662 – Facsimile
Email: craig@clalegal.com

William B. Federman (pro hac vice forthcoming)
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, OK 73120
Telephone: (405) 235-1560
-and-
212 W. Spring Valley Road
Richardson, TX 75081

Counsel for the Plaintiff and the Proposed Class