**UNITED STATES DISTRICT COURT**
**EASTERN DISTRICT OF VIRGINIA**
**RICHMOND DIVISION**

| | |
|---|---|
| **ALI MGARESH** and **JEFFREY MINTER**, on behalf of themselves and all others similarly situated,<br><br>Plaintiffs,<br><br>v.<br><br>**VIRGINIA UNION UNIVERSITY**,<br><br>Defendant. | Case No. 24-cv-337<br><br>**CLASS ACTION COMPLAINT**<br><br>**DEMAND FOR JURY TRIAL** |

Ali Mgaresh and Jeffrey Minter ("Plaintiffs"), through their attorneys, individually and on behalf of all others similarly situated, bring this Class Action Complaint against Defendant Virginia Union University ("VUU" or "Defendant"), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiffs allege the following on information and belief—except as to their own actions, counsel's investigations, and facts of public record.

## NATURE OF ACTION

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

2. Defendant is "a premier liberal arts urban institution of higher education"[1] located in Richmond, Virginia. In the 2023-24 academic year, over 1,200 undergraduate and 400 graduate students enrolled at VUU.[2] And in 2023, Defendant had approximately $51 million in revenue.[3]

3. As such, Defendant stores a litany of highly sensitive personal information—which was exposed when cybercriminals infiltrated Defendant's insufficiently protected computer systems in a data breach (the "Data Breach").

4. The Data Breach resulted in unauthorized disclosure, exfiltration, and theft of former, current, and prospective students' highly personal information, including full names, Social Security numbers, dates of birth, and Driver's License numbers or State ID information ("personally identifying information" or "PII").[4]

5. VUU's Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell its former, current, and prospective students how many people were impacted, exactly when the breach occurred, how the breach happened, or why VUU delayed notifying victims that hackers had gained access to highly sensitive PII.

6. On information and belief, Defendant detected the Data Breach on February 13, 2023.[5] However, Defendant did not provide notice to victims until more than *fourteen months* later.

---

[1] *Who We Are,* Virginia Union University, https://www.vuu.edu/about-union/about (last visited May 8, 2024).
[2] *Virginia Union University Celebrates 31% Enrollment Surge For 2023-24*, Virginia Union University, https://www.vuu.edu/news/vuu-celebrates-31-enrollment-surge (last visited May 8, 2024).
[3] Virginia Union University, ProPublica, https://projects.propublica.org/nonprofits/organizations/540524516 (last visited May 8, 2024).
[4] Notice Regarding a Data Security Incident, Viginia Union University, https://www.vuu.edu/Content/Uploads/vuu.edu/images/2024/docs/Pages%20from%20Sub%20Notice%20-%20VUU%20(final)(33531889.1)%20(003).pdf (last visited May 8, 2024).
[5] *Id.*

7. It is unknown precisely how long the cybercriminals had access to Defendant's network before the breach was discovered. In other words, Defendant had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to its current, former, and prospective students' PII.

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

9. Plaintiffs are Data Breach victims, having received a breach notice—an example is attached as Exhibit A ("Notice of Data Breach". They bring this class action on behalf of themselves, and all others harmed by Defendant's misconduct.

10. The exposure of one's PII to cybercriminals is a bell that cannot be unrung. Before this data breach, current, former and prospective students' private information was exactly that—private. Not anymore. Now, their private information is forever exposed and unsecure.

**PARTIES**

11. Plaintiff, Ali Mgaresh, is a natural person and citizen of New York. He resides in Brooklyn, New York where he intends to remain.

12. Plaintiff, Jeffrey Minter, is a natural person and citizen of Virginia. He resides in Cumberland, Virginia where he intends to remain.

13. Defendant, Virginia Union University, is a Virginia Nonstock Corporation with its principal place of business at 1500 N. Lombardy St., Richmond, Virginia 23220. The registered agent for Defendant is CT Corporation System at 4701 Cox Rd., Suite 285, Glen Allen, Virginia 23060.

## JURISDICTION AND VENUE

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

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

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

## BACKGROUND

***Defendant Collected and Stored the PII of Plaintiffs and the Class***

17. Defendant is "a premier liberal arts urban institution of higher education"[6] located in Richmond, Virginia. In the 2023-24 academic year, over 1,200 undergraduate and 400 graduate students enrolled at VUU.[7] And in 2023, Defendant had approximately $51 million in revenue.[8]

18. As part of its business, Defendant receives and maintains the PII of thousands of its current, former, and prospective students.

19. On information and belief, VUU maintains current, former, and prospective students' PII for years—even decades—after their relationship is terminated.

---

[6] *Who We Are,* Virginia Union University, https://www.vuu.edu/about-union/about (last visited May 8, 2024).
[7] *Virginia Union University Celebrates 31% Enrollment Surge For 2023-24*, Virginia Union University, https://www.vuu.edu/news/vuu-celebrates-31-enrollment-surge (last visited May 8, 2024).
[8] Virginia Union University, ProPublica, https://projects.propublica.org/nonprofits/organizations/540524516 (last visited May 8, 2024).

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

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

22. Defendant recognizes these duties, declaring in its "Notice Regarding a Data Security Incident" that:

a. "The privacy and security of personal information that Virginia Union University ("VUU") maintains is of the utmost importance;" and

b. It is "fully committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it."[9]

23. Additionally, defendant's FERPA policy notes that students have "[t]he right to consent to disclosures of personally identifiable information contained in the student's education records," acknowledging that current, former, and prospective students' PII should not be unauthorizedly disclosed.[10]

***Defendant's Data Breach***

24. On February 13, 2023, Defendant "detected unauthorized access within [its] network environment." Ex. A.

---

[9] Notice Regarding a Data Security Incident, Virginia Union University, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.vuu.edu/Content/Uploads/vuu.edu/images/2024/docs/Pages%20from%20Sub%20Notice%20-%20VUU%20(final)(33531889.1)%20(003).pdf

[10] FERPA Policy, Virginia Union University, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.vuu.edu/Content/Uploads/vuu.edu/files/FERPA.pdf

25. Worryingly, Defendant already admitted that Plaintiffs' and the Class' PII was actually stolen during the Data Breach, confessing that files were "subject to unauthorized access or acquisition." Ex. A.

26. Thus far, Defendant has refused to disclose the scope of the Data Breach. Specifically, Defendant has refused to disclose:

a. When the data breach occurred, and

b. Who was exposed in the Data Breach (e.g., students, employees, and/or consumers).

27. On information and belief—and based on the notice provided on Defendant's website—Defendant's Data Breach exposed *at least* the following types of PII:

a. names;

b. dates of birth;

c. Social Security numbers; and

d. Driver's license numbers or State ID numbers.

28. On information and belief, the exact scope of the Data Breach can be determined from information within Defendant's possession, custody, and/or control.

29. While the exact number of persons injured is currently unknown, upon information and belief, the size of the putative class can be ascertained from information in Defendant's custody and control. On information and belief, the putative class is over one hundred members—as it includes its current, former, and prospective students.

30. Furthermore, Defendant has not disclosed *when* the Data Breach began. Defendant has only disclosed when *they discovered* the Data Breach. Thus, upon information and belief, the Data Breach began prior to February 23, 2023. Ex. A.

31. Stunningly, Defendant waited until May 1, 2024, before it began notifying the class—a full fourteen months *after* Defendant discovered its Data Breach. Ex. A.

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

33. Defendant's Notice of Data Breach acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, encouraging Plaintiffs and the Class to:

a. "Plac[e] a fraud alert and/or security freeze on their credit files;"

b. "obtain[] a free credit report;"

c. "remain vigilant in reviewing their financial account statements, explanation of benefits statements and credit reports for fraudulent or irregular activity on a regular basis;" and

d. "report any suspicious activity to the proper authorities." Ex. A.

34. Defendant breached its duties by implementing inadequate security practices which ultimately caused the Data Breach and led to widespread injury and monetary damages. In other words, Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

35. Since the breach, Defendant has promised that it is "continually evaluating and modifying its practices and internal controls." Ex. A. But this is too little too late. Simply put, these measures—which Defendant now recognizes as necessary—should have been implemented *before* the Data Breach.

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

37. Further, the Notice of Data Breach shows that Defendant still has not determined the full scope of the Data Breach, as Defendant has not identified precisely what information was stolen and when.

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

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

***LockBit claims credit for the Data Breach***

40. Worryingly, the cybercriminals that obtained Plaintiffs' and Class members' PII appear to be the notorious Russian cybercriminal group "LockBit."[11]

41. Arising in Russia during early 2020, LockBit is now "the most deployed ransomware variant across the world and continues to be prolific in 2023."[12]

42. Thus, the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), the Multi-State Information Sharing and Analysis Center (MS-ISAC) have warned that:

[11] *Lockbit3*, RANSOMLOOK, https://www.ransomlook.io/group/lockbit3 (last visited May 8, 2024).
[12] *Cybersecurity Advisory*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (June 14, 2023) https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a (last visited May 8, 2024).

a. "LockBit affiliates have employed double extortion by first encrypting victim data and then exfiltrating that data while threatening to post that stolen data on leak sites."[13]

b. "Up to the Q1 2023, a total of 1,653 alleged victims were observed [i.e., published] on LockBit leak sites."[14]

43. And Reuters reports that:

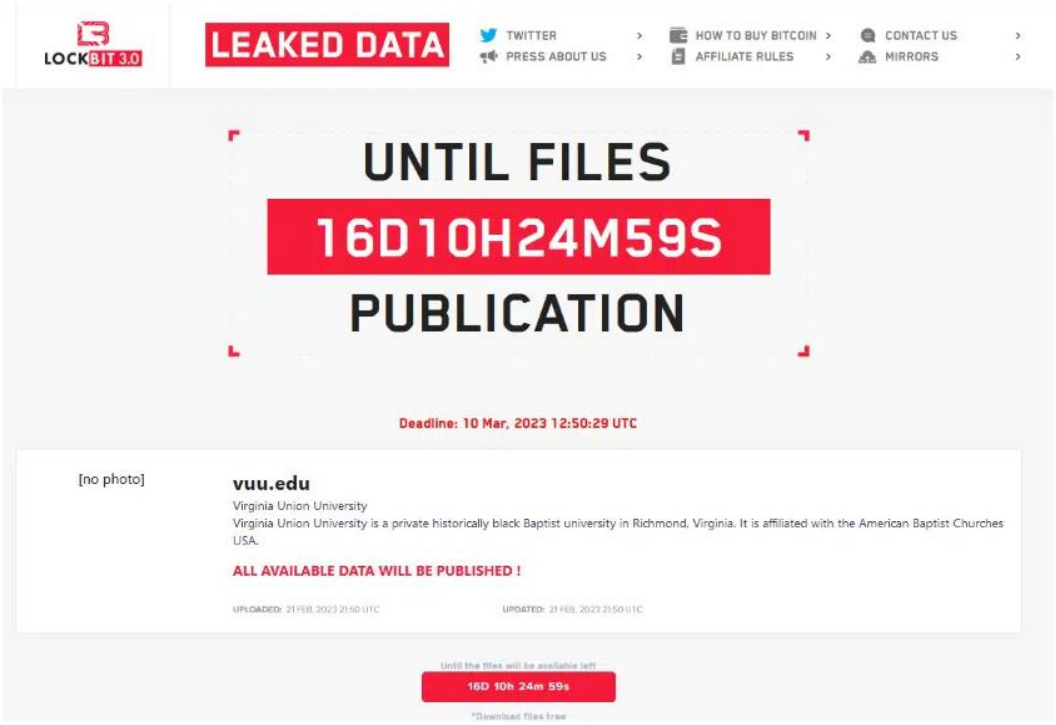
a. "On the dark web, Lockbit's blog displays an ever-growing gallery of victim organisations that is updated nearly daily."[15]

b. "Next to their names are digital clocks showing the number of days left to the deadline given to each organisation to provide ransom payment, failing which, the gang publishes the sensitive data it has collected."[16]

44. Here, LockBit claimed responsibility for Defendant's Data Breach—and then promised to ***publish*** the stolen PII/PH.[17] Specifically, LockBit promised that "ALL AVAILABLE DATA WILL BE PUBLISHED" on March 10, 2023.[18]

---

[13] *Id*.
[14] *Id*.
[15] Zeba Siddiqui & James Pearson, *Explainer: What is Lockbit? The digital extortion gang on a cybercrime spree*, REUTERS (Nov. 10, 2023) https://www.reuters.com/technology/cybersecurity/what-is-lockbit-digital-extortion-gang-cybercrime-spree-2023-11-10/.
[16] *Id*.
[17] *Virginia Union University Notifying People of Data Breach Following Cyber Attack I February 2023*, COMPARITECH, https://www.comparitech.com/news/virginia-union-university-notifying-people-of-data-breach-following-cyber-attack-in-february-2023/ (last visited May 8, 2024).
[18] *Id*.




| Group | Title | Date |
|---|---|---|
| Lockbit3 | vuu.edu | 2023-02-22 |
| Virginia Union University Virginia Union University is a private historically black Baptist university in Richmond, Virginia. It is affiliated with the American Baptist Churches USA. | | |

45. Thereafter, cybersecurity news reporters confirmed that the VUU Data Breach "was claimed by the LockBit ransomware gang at the time."[19]

46. Thus, on information and belief, Plaintiffs' and the Class's stolen PII has already been published (or will be published imminently) by LockBit on the Dark Web.

***Plaintiff Mgaresh's Experiences and Injuries***

47. Plaintiff Ali Mgaresh applied to be a student at VUU in approximately 2010-2011.

[19] *The Week in Ransomware: May 3, 2024*, COMPARITECH, https://www.comparitech.com/news/the-week-in-ransomware-may-3-2024/ (last visited May 8, 2024).

48. Thus, Defendant obtained and maintained Plaintiffs' PII.

49. As a result, Plaintiff was injured by Defendant's Data Breach.

50. As a condition of his application to VUU, Plaintiff was required to provide Defendant with his PII. Defendant used that PII to facilitate its educational services and required Plaintiff to provide that PII in order to obtain educational services.

51. Plaintiff provided his PII to Defendant and trusted VUU would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiffs' PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

52. Plaintiff reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of PII.

53. Plaintiff received a Notice of Data Breach in June 2023.

54. Thus, on information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

55. Through its Data Breach, Defendant compromised Plaintiffs':

a. name; and

b. Social Security number.

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

57. And in the aftermath of the Data Breach, Plaintiff has suffered from a spike in spam and scam text messages.

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

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

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

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

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

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

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

***Plaintiff Minter's Experiences and Injuries***

65. Plaintiff previously applied to be a student at VUU.

66. Thus, Defendant obtained and maintained Plaintiffs' PII.

67. As a result, Plaintiff was injured by Defendant's Data Breach.

68. As a condition of his application to VUU, Plaintiff was required to provide Defendant with his PII. Defendant used that PII to facilitate its educational services and required Plaintiff to provide that PII in order to obtain educational services.

69. Plaintiff provided his PII to Defendant and trusted VUU would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiffs' PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

70. Plaintiff reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of PII.

71. Plaintiff received a Notice of Data Breach in June 2023.

72. Thus, on information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

73. Through its Data Breach, Defendant compromised Plaintiffs':

a. name; and

b. Social Security number.

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

75. And in the aftermath of the Data Breach, Plaintiff has suffered from a dramatic spike in spam and scam text messages, calls, and emails.

76. Additionally, following the Data Breach, Plaintiff has suffered multiple instances of fraud in the form of unauthorized packages being delivered to his house.

77. Recently, an unauthorized actor fraudulently purchased an Audi in Plaintiffs' name and Plaintiff has since had multiple parking tickets delivered to his home address.

78. Following the Data Breach, Plaintiff has been alerted that there have been unauthorized credit inquiries on his credit report.

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

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

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

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

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

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

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

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

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

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

b. diminution in value of their PII;

c. compromise and continuing publication of their PII;

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

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

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII; and

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

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

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

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

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

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

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

93. Defendant disclosed the PII of Plaintiffs and Class members for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiffs and Class members to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and

fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

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

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

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

96. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the academic/education industries preceding the date of the breach.[20]

97. In light of recent high profile data breaches at other academic institutions, Defendant knew or should have known that its current, former, and prospective students' PII would be targeted by cybercriminals.

98. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[21] The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.[22]

---

[20] 6 Industries Most Affected by Security Breaches, Cobalt, https://www.cobalt.io/blog/industries-most-affected-by-security-breaches (last visited May 8, 2024).

[21] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.

[22] *Id.*

99. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack.

100. Cyberattacks have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."[23]

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

***Defendant Failed to Follow FTC Guidelines***

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

103. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[24] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

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

[23] Gordon M. Snow Statement, FBI https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector (last visited May 8, 2024).

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

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

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

105. Furthermore, the FTC explains that companies must:

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

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

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

106. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

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

***Defendant Failed to Follow Industry Standards***

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

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

110. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

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

***Defendant Violated HIPAA***

112. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly

known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[25]

113. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[26]

114. The Data Breach itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

[25] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[26] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

d. failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

115. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Defendant failed to comply with safeguards mandated by HIPAA regulations.

**CLASS ACTION ALLEGATIONS**

116. Plaintiffs bring this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and 23(b)(3),

individually and on behalf of all members of the following class:

> All individuals residing in the United States whose PII was compromised in the Data Breach discovered by Virginia Union University in February 2023, including all those individuals who received notice of the breach.

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

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

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

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

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

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

123. Adequacy. Plaintiffs will fairly and adequately protect the proposed Class's common interests. Their interests do not conflict with Class members' interests. And Plaintiffs

have retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

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

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

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

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

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

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

f. if Defendant's Breach Notice was reasonable;

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

h. what the proper damages measure is; and

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

125. Superiority. A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by

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

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

126. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

127. Plaintiffs and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their PII, use their PII for education and/or business purposes only, and/or not disclose their PII to unauthorized third parties.

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

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

130. Defendant owed these duties to Plaintiffs and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew

or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiffs and Class members' PII.

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

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

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

c. promptly detect attempts at unauthorized access;

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

132. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiffs and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs and Class members to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

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

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

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

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

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

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

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

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

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

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

141. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal

information and PII of Plaintiffs and Class members which actually and proximately caused the Data Breach and Plaintiffs and Class members' injury.

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

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

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

145. On information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

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

## SECOND CAUSE OF ACTION
**Negligence *per se***
**(On Behalf of Plaintiffs and the Class)**

147. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

148. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' PII.

149. 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 the PII entrusted to it. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs and the Class members' sensitive PII.

150. Defendant breached its respective duties to Plaintiffs and Class members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

151. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect 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 had 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.

152. 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 businesses 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 Plaintiffs and members of the Class.

153. But for Defendant's wrongful and negligent breach of its duties owed, Plaintiffs and Class members would not have been injured.

154. The injury and harm suffered by Plaintiffs and Class members was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that Defendant was failing to meet its duties and that its breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

155. Similarly, under HIPAA, Defendant had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiffs' and Class members' PHI.

156. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect its PHI and by not complying with applicable regulations detailed *supra*. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of PHI that 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.

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

158. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class members have suffered and will continue to suffer numerous injuries (as detailed *supra*).

## THIRD CAUSE OF ACTION
**Breach of Implied Contract**
**(On Behalf of Plaintiffs and the Class)**

159. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

160. Plaintiffs and Class members were required to provide their PII to Defendant as a condition of receiving services provided by Defendant. Plaintiffs and Class members provided their PII to Defendant or its third-party agents in exchange for Defendant's services.

161. Plaintiffs and Class members reasonably understood that a portion of the funds they paid Defendant (or of the funds derived from their labor) would be used to pay for adequate cybersecurity measures.

162. Plaintiffs and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

163. Plaintiffs and the Class members accepted Defendant's offers by disclosing their PII to Defendant or its third-party agents in exchange for services.

164. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII to unauthorized persons.

165. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiffs' and Class Member's PII.

166. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and Class members with prompt and adequate notice of all unauthorized access and/or theft of their PII.

167. After all, Plaintiffs and Class members would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

168. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

169. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain.

In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

170. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

171. Defendant materially breached the contracts it entered with Plaintiffs and Class members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII that Defendant created, received, maintained, and transmitted.

172. In these and other ways, Defendant violated its duty of good faith and fair dealing.

173. Defendant's material breaches were the direct and proximate cause of Plaintiffs' and Class members' injuries (as detailed *supra*).

174. On information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

175. Plaintiffs and Class members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

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

176. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

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

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

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

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

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

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

**FIFTH CAUSE OF ACTION**
**Invasion of Privacy**
**(On Behalf of Plaintiffs and the Class)**

183. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

184. Plaintiffs and the Class had a legitimate expectation of privacy regarding their highly sensitive and confidential PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

185. Defendant owed a duty to its current, former, and prospective students, including Plaintiffs and the Class, to keep this information confidential.

186. The unauthorized acquisition (i.e., theft) by a third party of Plaintiffs and Class members' PII is highly offensive to a reasonable person.

187. The intrusion was into a place or thing which was private and entitled to be private. Plaintiffs and the Class disclosed their sensitive and confidential information to Defendant, but did so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

188. The Data Breach constitutes an intentional interference with Plaintiffs' and the Class's interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

189. Defendant acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

190. Defendant acted with a knowing state of mind when it failed to notify Plaintiffs and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

191. Acting with knowledge, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

192. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiffs and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages (as detailed *supra*).

193. On information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

194. Unless and until enjoined and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII are still maintained by Defendant with their inadequate cybersecurity system and policies.

195. Plaintiffs and the Class have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiffs and the Class.

196. In addition to injunctive relief, Plaintiffs, on behalf of themselves and the other Class members, also seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest and costs.

## SIXTH CAUSE OF ACTION
### Unjust Enrichment
### (On Behalf of Plaintiffs and the Class)

197. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

198. This claim is pleaded in the alternative to the breach of implied contract claim.

199. Plaintiffs and Class members conferred a benefit upon Defendant. After all, Defendant benefitted from using their PII to provide services.

200. Defendant appreciated or had knowledge of the benefits it received from Plaintiffs and Class members. And Defendant benefited from receiving Plaintiffs' and Class members' PII, as this was used to provide services.

201. Plaintiffs and Class members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

202. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class members' PII.

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

204. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and Class members' payment because Defendant failed to adequately protect their PII.

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

206. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiffs and Class members—all unlawful or inequitable proceeds that it received because of its misconduct.

**SEVENTH CAUSE OF ACTION**
**Declaratory Judgment**
**(On Behalf of Plaintiffs and the Class)**

207. Plaintiffs incorporate by reference all other paragraphs as if fully set forth herein.

208. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. The Court has broad authority to restrain acts, such as those alleged herein, which are tortious and unlawful.

209. In the fallout of the Data Breach, an actual controversy has arisen about Defendant's various duties to use reasonable data security. On information and belief, Plaintiffs allege that Defendant's actions were—and *still* are—inadequate and unreasonable. And Plaintiffs and Class members continue to suffer injury from the ongoing threat of fraud and identity theft.

210. Given its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Defendant has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Defendant breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Defendant breaches of its duties caused—and continues to cause—injuries to Plaintiffs and Class members.

211. The Court should also issue corresponding injunctive relief requiring Defendant to use adequate security consistent with industry standards to protect the data entrusted to it.

212. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy if Defendant experiences a second data breach.

213. And if a second breach occurs, Plaintiffs and the Class will lack an adequate remedy at law because many of the resulting injuries are not readily quantified in full and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages—while warranted for out-of-pocket damages and other legally quantifiable and provable damages—cannot cover the full extent of Plaintiffs and Class members' injuries.

214. If an injunction is not issued, the resulting hardship to Plaintiffs and Class members far exceeds the minimal hardship that Defendant could experience if an injunction is issued.

215. An injunction would benefit the public by preventing another data breach—thus preventing further injuries to Plaintiff, Class members, and the public at large.

**PRAYER FOR RELIEF**

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

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

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

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

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

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

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

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

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

I. Granting other relief that this Court finds appropriate.

**DEMAND FOR JURY TRIAL**

Plaintiffs demand a jury trial for all claims so triable.

Date: May 13, 2024

Respectfully submitted,

By: /s/ David Hilton Wise
David Hilton Wise, VSB No. 30828
**WISE LAW FIRM, PLC**
10640 Page Street, Ste 320
Fairfax, Virginia 22030
Tel: (703) 934-6377
Fax: (703) 934-6379
dwise@wiselaw.pro

Samuel J. Strauss*
Cassandra P. Miller*
**STRAUSS BORRELLI LLP**
One Magnificent Mile
980 N. Michigan Avenue, Suite 1610
Chicago, IL, 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com

**pro hac vice forthcoming*

*Attorneys for Plaintiffs and Proposed Class*