

**STATE OF MICHIGAN**  
**IN THE THIRTY-SEVENTH CIRCUIT COURT FOR THE COUNTY OF CALHOUN**

|                                                                                                                                                                                                                                  |                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <p>MATTHEW LANE AND ZACHARY KNAPP, <i>on behalf of themselves and all others similarly situated</i>,</p> <p style="text-align:right">Plaintiffs,</p> <p>v.</p> <p>ALBION COLLEGE,</p> <p style="text-align:right">Defendant.</p> | <p>Case No. 25-1301-NZ</p> <p>Hon. John A. Hallacy</p> <p><b>FIRST AMENDED CLASS ACTION COMPLAINT</b></p> <p><b>JURY TRIAL DEMANDED</b></p> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|

David H. Fink (P28235)  
Nathan J. Fink (P75185)  
FINK BRESSACK  
38500 Woodward Ave, Suite 350  
Bloomfield Hills, MI 48304  
Telephone: (248) 971-2500  
dfink@finkbressack.com  
nfink@finkbressack.com

Leanna Loginov\*  
SHAMIS & GENTILE, P.A.  
14 NE First Avenue, Suite 705  
Miami, Florida 33132  
Telephone: 305-479-2299  
lloginov@shamisgentile.com

Raina C. Borrelli\*  
STRAUSS BORRELLI PLLC  
980 N. Michigan Avenue, Suite 1610  
Chicago, Illinois 60611  
Telephone: (872) 263-1100  
raina@straussborrelli.com

*Counsel for Plaintiffs and the Putative Class*

*\*Application for pro hac forthcoming*

Kylie E. Stryffeler (P83006)  
BRICKER GRAYDON LLP  
100 South 3rd St.  
Columbus, Ohio 43215  
Telephone: (614) 227-4892  
kstryffeler@brickkergraydon.com

*Counsel for Defendant, Albion College*

There is no pending or resolved civil action arising out of the transactions or occurrences alleged in this Complaint.

## **FIRST AMENDED CLASS ACTION COMPLAINT**

Plaintiffs Matthew Lane and Zachary Knapp (“Plaintiffs”) bring this Class Action Complaint (“Complaint”) against Defendant Albion College (“Defendant” or “Albion College”) individually and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsel’s investigation, and upon information and belief as to all other matters, as follows:

### **NATURE OF THE ACTION**

1. This class action arises out of the recent data breach (“Data Breach”) involving Defendant, a nonprofit liberal arts college.

2. Plaintiffs bring this Complaint against Defendant for its failure to properly secure and safeguard the personally identifiable information that it collected and maintained as part of its regular business practices, including Plaintiffs’ and Class Members’ names, Social Security numbers, and bank account information (collectively defined herein as “Private Information”).

3. Upon information and belief, current/former employees and current/former students of Defendant are required to entrust Defendant with sensitive, non-public Private Information, without which Defendant could not perform its regular business activities. Defendant retains this information for at least many years and even after the employee-employer and/or student-school relationship has ended.

4. By obtaining, collecting, using, and deriving a benefit from the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

5. Defendant failed to adequately protect Plaintiffs’ and Class Members’ Private Information—and failed to even encrypt or redact this highly sensitive information. This

unencrypted, unredacted Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and its utter failure to protect Plaintiffs' and Class Members' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk of identity theft and fraud to victims of the Data Breach will remain for their respective lifetimes.

6. In breaching its duties to properly safeguard Plaintiffs' and Class Members' Private Information and give them timely, adequate notice of the Data Breach's occurrence, Defendant's conduct amounts to negligence and/or recklessness and violates federal and state statutes.

7. Plaintiffs bring this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

8. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the Private Information of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the Private Information of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and

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

9. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) invasion of their privacy; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

10. Plaintiffs seek to remedy these harms and prevent any future data compromise on behalf of themselves and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate data security practices.

## **PARTIES**

11. Plaintiff Matthew Lane is a natural resident and citizen of Michigan.

12. Plaintiff Zachary Knapp is a natural resident and citizen of Michigan.

13. Defendant is a nonprofit corporation organized under the state laws of Michigan with its principal place of business located in Albion, Michigan.

## **JURISDICTION AND VENUE**

14. This is an action asserting class claims for damages and declaratory relief pursuant to MCR 3.501.

15. The amount in controversy exceeds \$25,000, exclusive of interest costs and attorneys' fees. Plaintiffs do not currently know if the total amount in controversy exceeds \$5 million.

16. This Court has personal jurisdiction over Albion because Defendant is domiciled in the State of Michigan and regularly conducts and/or solicits business in, engages in other persistent courses of conduct in, and/or derives substantial revenue from products and/or services provided to persons in this County.

17. Venue is proper in this County because Defendant has its principal place of business in Calhoun County and regularly conducts business in Calhoun County.

## **FACTUAL ALLEGATIONS**

### ***Background of Defendant.***

18. Defendant is a nonprofit liberal arts college in Albion, Michigan.

19. Plaintiffs and Class Members are current/former employees and current/former students of Defendant.

20. As a condition of employment and/or enrollment with Albion College, Plaintiffs and Class Members were required to provide Defendant with their sensitive and confidential Private Information, including their names, Social Security numbers, and bank account information.

21. The information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted Private Information of Plaintiffs and Class Members.

22. Upon information and belief, Defendant made promises and representations to its current/former employees and current/former students, including Plaintiffs and Class Members, that the Private Information collected from them as a condition of employment and/or enrollment would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

23. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

24. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

25. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep its clients' employees' Private Information safe and confidential.

26. Defendant recognized these duties in its "Data Privacy Policy," promising:

- a. "Albion College ("the College") is committed to maintaining the privacy, integrity, security and availability of confidential information created, received, maintained and/or stored by the College, regardless of form;"

- b. “Confidential information and records are to be accessed, used and disclosed only with explicit authorization, in accordance with applicable law, and on a need-to-know basis related to a College function. Such information must never be disclosed outside of the College without express authorization;”
- c. “To help users appropriately secure and manage Confidential information and records, the College has adopted various Data Standards set by the State of Michigan ([safecomputing.umich.edu](https://safecomputing.umich.edu)), that, among other things, categorizes data by sensitivity and risk level and designates roles and responsibilities for data use and management.”<sup>1</sup>

27. Despite recognizing its duty to do so, on information and belief, Albion did not implement reasonably cybersecurity safeguards or policies to protect its employees’ and students’ PII or supervise its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, Albion leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to the PII in its possession.

28. Defendant had obligations created by FTC Act, contract, industry standards, and representations made to Plaintiffs and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

29. Defendant derived a substantial economic benefit from collecting Plaintiffs’ and Class Members’ Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

---

<sup>1</sup> *Data Privacy Policy*, ALBION COLLEGE, <https://www.albion.edu/offices/information-technology/support/data-privacy-policy/> (last visited May 12, 2025).

30. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

***The Data Breach.***

31. Starting on or about May 1, 2025, Defendant began sending Plaintiffs and other victims of the Data Breach a letter (the "Notice Letter"), informing them that:

**What Happened?** We recently discovered unauthorized access to our network occurred on December 17, 2024.

**What Information Was Involved?** Based on our comprehensive investigation and document review, which concluded on April 18, 2025, we discovered that your full name and one or more of the following were removed from our network in connection with this incident: Social Security Number; bank account information.<sup>2</sup>

32. Additionally, Defendant reported to the Attorney General of Texas that the below types of PII were compromised in the Data Breach:

- a. Social Security numbers.
- b. Government issued ID numbers (e.g. passport, state ID card),
- c. Financial Information (e.g. account number, credit or debit card number), and
- d. Medical Information.<sup>3</sup>

33. Omitted from the Notice Letter were the identity of the cybercriminals who perpetrated this Data Breach, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To

---

<sup>2</sup> The "Notice Letter", attached hereto as ***Exhibit A***.

<sup>3</sup> *Data Security Breach Reports*, ATTORNEY GENERAL OF TEXAS, <https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage> (last visited June 29, 2025).

date, these critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

34. This “disclosure” amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class Members of the Data Breach’s critical facts. Without these details, Plaintiffs’ and Class Members’ ability to mitigate the harms resulting from the Data Breach is severely diminished.

35. Despite Defendant’s intentional opacity about the root cause of this incident, several facts may be gleaned from the Notice Letter, including: a) that this Data Breach was the work of cybercriminals; b) that the cybercriminals first infiltrated Defendant’s networks and systems, and downloaded data from the networks and systems (aka exfiltrated data, or in layperson’s terms “stole” data; and c) that once inside Defendant’s networks and systems, the cybercriminals targeted information including Plaintiffs’ and Class Members’ names, Social Security numbers, and bank account information for download and theft.

36. To be clear – there are numerous issues with Albion College’s Data Breach, but the deficiencies in the Data Breach notification letter exacerbate the circumstances for victims of the Data Breach: (1) Albion College waited over *four* months to notice Plaintiffs and Class members of the Data Breach; (2) Albion College fails to state whether it was able to contain or end the cybersecurity threat, leaving victims to fear whether the Private Information that Albion College continues to maintain is secure; and (3) Albion College fails to state how the breach itself occurred. All of this information is vital to victims of a data breach, let alone a data breach of this magnitude due to the sensitivity and wide array of information compromised in this specific breach.

37. Moreover, in its Notice Letter, Defendant failed to specify whether it undertook any efforts to contact the Class Members whose data was accessed and acquired in the Data Breach

to inquire whether any of the Class Members suffered misuse of their data, whether Class Members should report their misuse to Defendant, and whether Defendant set up any mechanism for Class Members to report any misuse of their data.

38. Furthermore, Defendant's delay in notifying Plaintiffs and Class members of the Data Breach is in direct violation of Defendant's responsibilities under the data breach notification statute in Michigan. See MCL 445.72 which requires that the disclosure notification be made "without unreasonable delay"<sup>4</sup>.

39. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiffs and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

40. The attacker targeted, accessed, and acquired files in Defendant's computer systems containing unencrypted Private Information of Plaintiffs and Class Members, including their names, Social Security numbers, and bank account information. Plaintiffs' and Class Members' Private Information was accessed and stolen in the Data Breach.

41. Plaintiffs further believe that his Private Information and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

---

<sup>4</sup> While the definition of "reasonable" differs from state to state, the range is between 30-60 days. Defendant failed to meet this requirement by over **70 days**.

42. Indeed, numerous cybersecurity firms who track dark web activity have reported that the hacker group “Medusa” has taken credit for the Data Breach.<sup>5, 6</sup>

43. Medusa is a cyber gang that, according to the United States’ Cybersecurity and Infrastructure Security Agency (“CISA”), operates a double extortion model, where a organization’s files are encrypted and *exfiltrated* to Medusa’s servers.<sup>7</sup> Organizations then must pay to decrypt the stolen files and prevent their release.<sup>8</sup>

44. CISA further advises that Medusa has expanded to an “affiliate model” where affiliates, referred to as “Medusa actors,” use the group’s software to attack organizations and take a cut of the resulting extortion payments.<sup>9</sup>

45. On December 23, 2024, Medusa created a post on its dark web website<sup>10</sup> indicating that it had hacked Defendant and stolen PII from its computer network.<sup>11</sup>

---

<sup>5</sup> HACK TUESDAY WEEK 18 – 24 DECEMBER 2024, HACKMANAC, <https://hackmanac.com/news/hack-tuesday-week-18-24-december-2024> (last visited May 12, 2025).

<sup>6</sup> [MEDUSA] – Ransomware Victim: Albion College, REDPACKET SECURITY (Dec. 23, 2024), <https://www.redpacketsecurity.com/medusa-ransomware-victim-albion-college/>.

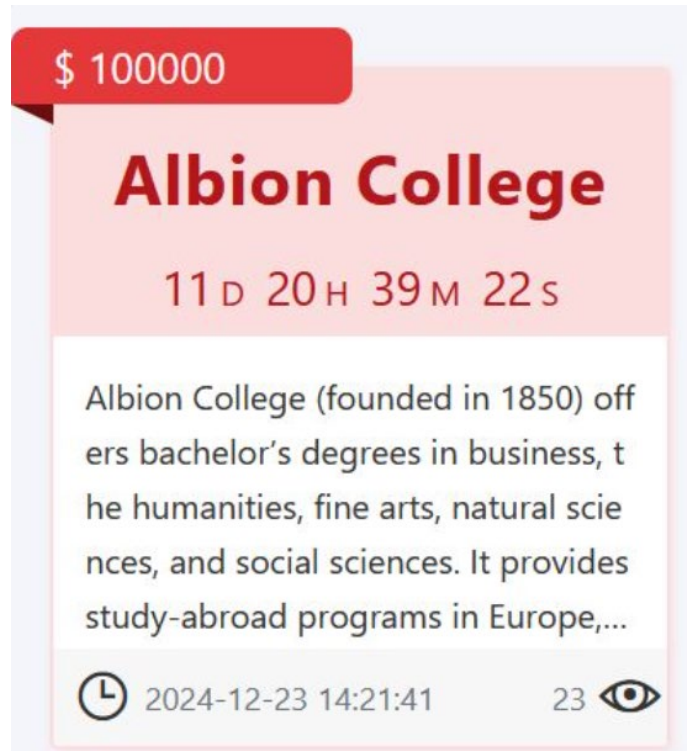
<sup>7</sup> #StopRansomware: Medusa Ransomware, CISA (Mar. 12, 2025), <https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a>.

<sup>8</sup> *Id.*

<sup>9</sup> *Id.*

<sup>10</sup> The screen shot regarding the dark web post related to the Data Breach was obtained from Falcon Feeds, a firm providing cybersecurity and dark web and ransomware monitoring services. See Home Page, FALCON FEEDS, <https://falconfeeds.io/> (last visited May 10, 2025).

<sup>11</sup> @FalconFeeds.io, Twitter (X) (December 23, 2024, 10:47 AM) <https://bsky.app/profile/falconfeedsio.bsky.social/post/3ldyf2p6lls2z>.



46. Medusa’s post listed a price of “\$100,000” and a countdown clock stating “11 D, 20 H, 39 M , 22 S” indicating Albion’s data would be published if Albion did not make a ransom payment within that time period.<sup>12</sup>

47. CISA has confirmed that this is Medusa’s *modus operandi*, stating in its advisory that “Medusa operates a [dark web] data leak site, divulging victims alongside countdowns to the release of information. Ransom demands are posted on the site, with direct hyperlinks to Medusa affiliated cryptocurrency wallets. At this stage, *Medusa concurrently advertises sale of the data to interested parties before the countdown timer ends*. Victims can additionally pay \$10,000 USD in cryptocurrency to add a day to the countdown timer.”<sup>13</sup>

---

<sup>12</sup> *Id.*

<sup>13</sup> #StopRansomware: Medusa Ransomware, CISA (Mar. 12, 2025), <https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a>. (emphasis added).

48. Defendant has not made any public statements on whether it made a ransom payment to Medusa related to the Data Breach.

49. Thus, on information and belief, Plaintiffs' and Class Members' PII has already been published, or will be published imminently, on the dark web.

50. Moreover, even if Albion made a ransom payment, there is no guarantee that the data Medusa stole will be deleted.<sup>14</sup> The stolen PII is valuable, and can easily be sold to another threat actor, so there is little incentive to delete it.<sup>15</sup> As the CISA advisory indicated *supra*, Medusa advertises the sale of the data it steals to anyone willing to pay concurrently with its ransom demands.

51. In addition, according to the CISA advisory, FBI investigations identified that after paying the ransom, one victim was contacted by a separate Medusa actor who claimed the negotiator had stolen the ransom amount already paid and requested half of the payment be made again to provide the "true decryptor."<sup>16</sup> This indicates that the "Medusa actors" will not abide by Medusa's promises not to disclose an organization's data after a ransom payment has been made.

52. Further, there have been cases where the links that lead to compromised files, while removed from the group who received the ransom payment's dark web website, remain available on the servers used by other hackers, even after the demand is met.<sup>17</sup>

53. Cybercriminal groups can monetize stolen PII and sell it on the dark web as part of

---

<sup>14</sup> Steve Adler, *Majority of Ransomware Victims That Pay a Ransom Suffer a Second Attack*, THE HIPAA JOURNAL (Feb. 23, 2024), <https://www.hipaajournal.com/majority-of-ransomware-victims-that-pay-a-ransom-suffer-a-second-attack/>.

<sup>15</sup> *Id.*

<sup>16</sup> #StopRansomware: Medusa Ransomware, CISA (Mar. 12, 2025), <https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-071a>.

<sup>17</sup> *Dedicated Leak Sites (DLS): Here's what you should know*, Group-IB, <https://www.group-ib.com/resources/knowledge-hub/dedicated-leak-sites/> (last visited Apr. 22, 2025).

a full identity profile.<sup>18</sup> Buyers can then use that information to conduct different types of identity theft or fraud, such as filing a fake tax return, applying for a fraudulent mortgage or opening a bank account while impersonating the victim.<sup>19</sup>

54. To date, on information and belief, Defendant has not notified Plaintiff and Class Members about the theft of their PII by Medusa, leaving them vulnerable to identity theft and fraud.

55. As a result of Albion's omissions, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach has been severely impaired.

56. Upon information and belief, the Medusa cybercriminal group was able to: (1) defeat Albion's security systems, (2) gain access to its network and gain access to the sensitive PII contained therein, and (3) successfully steal Plaintiffs' and the Class's PII.

57. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."<sup>20</sup>

58. Defendant, a sophisticated actor with that states it strives to ensure data integrity,<sup>21</sup> knew or should have known of the tactics that groups like Medusa employ.

---

<sup>18</sup> Anthony M. Freed, *Which Data Do Ransomware Attackers Target for Double Extortion?*, MALICIOUSLIFE BY CYBEREASON, <https://www.cybereason.com/blog/which-data-do-ransomware-attackers-target-for-double-extortion> (listed visited Mar. 6, 2025).

<sup>19</sup> *Id.*

<sup>20</sup> Brenda R. Sharton, *Your Company's Data Is for Sale on the Dark Web. Should You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) <https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back>.

<sup>21</sup> *Information Technology*, ALBION COLLEGE, <https://www.albion.edu/offices/information-technology/> (last visited May 12, 2025).

***Data Breaches Are Preventable.***

59. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

60. 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.”<sup>22</sup>

61. To prevent and detect cyber-attacks, Defendant could and should have implemented, as recommended by the United States Government, 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.

---

<sup>22</sup> 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> (last visited May 6, 2025).

- 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.<sup>23</sup>

62. To prevent and detect cyber-attacks or ransomware attacks, 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**

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

---

<sup>23</sup> *Id.* at 3-4.

### **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].<sup>24</sup>

63. Given that Defendant was storing the sensitive Private Information of its employees and current/former students, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

64. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and the exposure of the Private Information of, upon information and belief, thousands of thousands of individuals, including that of Plaintiffs and Class Members.

### ***Defendant Acquires, Collects, and Stores Plaintiffs' and Class Members' Private Information***

---

<sup>24</sup> 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/> (last visited May 6, 2025).

65. As a condition of employment and/or enrollment with Albion College, Plaintiffs and Class Members were required to give their sensitive and confidential Private Information to Defendant.

66. Defendant retains and stores this information and derives a substantial economic benefit from the Private Information that it collects. But for the collection of Plaintiffs' and Class Members' Private Information, Defendant would be unable to perform its services.

67. By obtaining, collecting, and storing the Private Information of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting the Private Information from disclosure.

68. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and relied on Defendant to keep their Private Information confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

69. Defendant could have prevented this Data Breach by properly securing and encrypting the files and file servers containing the Private Information of Plaintiffs and Class Members.

***Defendant Knew or Should Have Known of the Risk Because Companies in Possession of Private Information are Particularly Susceptible to Cyber Attacks.***

70. Data thieves regularly target companies like Defendant's due to the highly sensitive information that they custody. Defendant knew and understood that unprotected Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize that Private Information through unauthorized access.

71. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting entities that collect and store

Private Information and other sensitive information, like Defendant, preceding the date of the breach.

72. In 2023, an all-time high for data compromises occurred, with 3,205 compromises affecting 353,027,892 total victims.<sup>25</sup>

73. In light of recent high profile data breaches at other industry-leading companies, including T-Mobile, USA (37 million records, February-March 2023), 23andMe, Inc. (20 million records, October 2023), Wilton Reassurance Company (1.4 million records, June 2023), NCB Management Services, Inc. (1 million records, February 2023), Defendant knew or should have known that the Private Information that it collected and maintained would be targeted by cybercriminals.

74. Additionally, as companies became more dependent on computer systems to run their business,<sup>26</sup> e.g., working remotely as a result of the Covid-19 pandemic, and the Internet of Things (“IoT”), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.<sup>27</sup>

75. As a custodian of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiffs and Class Members as a result of a breach.

---

<sup>25</sup> See *2023 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2024); [https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC\\_2023-Annual-Data-Breach-Report.pdf](https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf). (last visited May 6, 2025).

<sup>26</sup> <https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html> (last visited May 6, 2025).

<sup>27</sup> <https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022> (last visited May 6, 2025).

76. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the Private Information of Plaintiffs and Class Members from being compromised.

77. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

78. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to more than six thousand individuals' detailed, Private Information, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data<sup>28</sup>.

79. In the Notice Letter, Defendant makes an offer of 12 months of identity monitoring services. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs and Class Members' Private Information. Moreover, once this service expires, Plaintiffs and Class Members will be forced to pay out of pocket for necessary identity monitoring services.

---

<sup>28</sup><https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/d16941f7-1e1e-4625-9a16-437a13f4f948.html> (last visited May 6, 2025).

80. Defendant's offering of credit and identity monitoring establishes that Plaintiffs and Class Members' sensitive Private Information *was* in fact affected, accessed, compromised, and exfiltrated from Defendant's computer systems.

81. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

82. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

83. As a company in possession of Plaintiffs' and Class Members' Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class Members and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Nevertheless, Defendant failed to take adequate cybersecurity measures to prevent the Data Breach.

***Value of Personally Identifying Information.***

84. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."<sup>29</sup> The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's

---

<sup>29</sup> 17 CFR § 248.201 (2013).

license or identification number, alien registration number, government passport number, employee-benefit management company or taxpayer identification number.”<sup>30</sup>

85. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.<sup>31</sup> For example, Personal Information can be sold at a price ranging from \$40 to \$200.<sup>32</sup> Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.<sup>33</sup>

86. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—name and Social Security number.

87. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”<sup>34</sup>

---

<sup>30</sup> *Id.*

<sup>31</sup> *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited May 6, 2025).

<sup>32</sup> *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited May 6, 2025).

<sup>33</sup> *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited May 6, 2025).

<sup>34</sup> Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited May 6, 2025).

88. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

89. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.<sup>35</sup>

90. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

***Defendant Fails to Comply with FTC Guidelines.***

91. 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.

92. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal employee information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer

---

<sup>35</sup> *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last visited May 6, 2025).

networks; understand their network's vulnerabilities; and implement policies to correct any security problems.<sup>36</sup>

93. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon 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.<sup>37</sup>

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

95. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect employee data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential employee data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 USC § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

96. These FTC enforcement actions include actions against companies in possession of Private Information, like Defendant.

---

<sup>36</sup> *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at [https://www.ftc.gov/system/files/documents/plain-language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last visited May 6, 2025).

<sup>37</sup> *Id.*

97. Section 5 of the FTC Act, 15 USC § 45, 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 Private Information. The FTC publications and orders described above also form part of the basis of Defendant’s duty in this regard.

98. Defendant failed to properly implement basic data security practices.

99. Defendant’s failure to employ reasonable and appropriate measures to protect against unauthorized access to employees’ Private Information or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 USC § 45.

100. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of its clients’ employees, Defendant was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant’s conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

***Defendant Fails to Comply with Industry Standards.***

101. As noted above, experts studying cyber security routinely companies in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

102. Several best practices have been identified that, at a minimum, should be implemented by companies in possession of Private Information, like Defendant, including but not limited to: 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. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

103. Other best cybersecurity practices that are standard for companies like Defendant 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; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

104. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR.DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

105. These foregoing frameworks are existing and applicable industry standards for companies in possession of Private Information to safeguard their employees' data, and upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

***Common Injuries and Damages.***

106. As a result of Defendant's ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession

of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) nominal damages; and (viii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

***The Data Breach Increases Victims' Risk of Identity Theft.***

107. The unencrypted Private Information of Plaintiffs and Class Members will end up for sale on the dark web as that is the *modus operandi* of hackers.

108. Unencrypted Private Information may also fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Simply put, unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

109. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

110. Plaintiffs’ and Class Members’ Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach has been used and will continue to be used in a variety of sordid ways for criminals to exploit Plaintiffs and Class Members and to profit off their misfortune.

111. Due to the risk of one’s Social Security number being exposed, state legislatures have passed laws in recognition of the risk: “[t]he social security number can be used as a tool to perpetuate fraud against a person and to acquire sensitive personal, financial, medical, and familial information, the release of which could cause great financial or personal harm to an individual. While the social security number was intended to be used solely for the administration of the federal Social Security System, over time this unique numeric identifier has been used extensively for identity verification purposes[.]”<sup>38</sup>

112. Moreover, “SSNs have been central to the American identity infrastructure for years, being used as a key identifier[.] . . . U.S. banking processes have also had SSNs baked into their identification process for years. In fact, SSNs have been the gold standard for identifying and verifying the credit history of prospective customers.”<sup>39</sup>

113. “Despite the risk of fraud associated with the theft of Social Security numbers, just five of the nation’s largest 25 banks have stopped using the numbers to verify a customer’s identity after the initial account setup[.]”<sup>40</sup> Accordingly, since Social Security numbers are frequently used to verify an individual’s identity after logging onto an account or attempting a transaction,

---

<sup>38</sup> See NC Gen Stat § 132-1.10(1).

<sup>39</sup> See <https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers> (last visited May 6, 2025).

<sup>40</sup> See <https://archive.nytimes.com/bucks.blogs.nytimes.com/2013/03/20/just-5-banks-prohibit-use-of-social-security-numbers/> (last visited May 6, 2025).

“[h]aving access to your Social Security number may be enough to help a thief steal money from your bank account”<sup>41</sup>

114. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of “Fullz” packages.<sup>42</sup>

115. With “Fullz” packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

116. The development of “Fullz” packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs’ and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still

---

<sup>41</sup> See <https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/> (last visited May 6, 2025).

<sup>42</sup> “Fullz” is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. See, e.g., Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), [https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-\]\(https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/](https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-) (last visited May 6, 2025).

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.

117. The existence and prevalence of “Fullz” packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like contact information) of Plaintiffs and the other Class Members.

118. Thus, even if certain information (such as contact information) was not stolen in the data breach, criminals can still easily create a comprehensive “Fullz” package.

119. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

***Loss of Time to Mitigate the Risk of Identity Theft and Fraud.***

120. As a result of the recognized risk of identity theft, when a Data Breach occurs, and an individual is notified by a company that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm – yet the resource and asset of time has been lost.

121. Thus, due to the actual and imminent risk of identity theft, Defendant, in its Notice Letter instructs Plaintiffs and Class Members to protect themselves by reviewing account statements and monitoring their credit reports, in addition to enrolling in the offered free credit monitoring program.

122. Defendant’s extensive suggestion of steps that Plaintiffs and Class Members must take in order to protect themselves from identity theft and/or fraud demonstrates the significant

time that Plaintiffs and Class Members must undertake in response to the Data Breach. Plaintiffs' and Class Members' time is highly valuable and irreplaceable, and accordingly, Plaintiffs and Class Members suffered actual injury and damages in the form of lost time that they spent on mitigation activities in response to the Data Breach and at the direction of Defendant's Notice Letter.

123. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach, freezing their payment cards, contacting credit bureaus to place freezes on their accounts, and monitoring their financial accounts for any indication of fraudulent activity, which may take years to detect. Accordingly, the Data Breach has caused Plaintiffs and Class Members to suffer actual injury in the form of lost time—which cannot be recaptured—spent on mitigation activities.

124. Plaintiffs' mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."<sup>43</sup>

125. Plaintiffs' mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity),

---

<sup>43</sup> See United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), <https://www.gao.gov/new.items/d07737.pdf>. (last visited May 6, 2025).

reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.<sup>44</sup>

126. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time to repair the damage to their good name and credit record.”<sup>[4]</sup>

***Diminution of Value of Private Information.***

127. Private Information is a valuable property right.<sup>45</sup> Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

128. Sensitive Private Information can sell for as much as \$363 per record according to the Infosec Institute.<sup>46</sup>

129. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly \$200 billion.<sup>47</sup> In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data

---

<sup>44</sup> See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps> (last visited May 6, 2025).

<sup>45</sup> See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” p. 2, U.S. Government Accountability Office, June 2007, <https://www.gao.gov/new.items/d07737.pdf> (last visited May 6, 2025) (“GAO Report”).

<sup>46</sup> See, e.g., John T. Soma, et al, Corporate Privacy Trend: The “Value” of Personally Identifiable Information (“PII”) Equals the “Value” of Financial Assets, 15 Rich. J.L. & Tech. 11, at \*3-4 (2009) (“PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations omitted). (last visited May 6, 2025).

<sup>47</sup> See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last visited May 6, 2025).

broker who in turn aggregates the information and provides it to marketers or app developers.<sup>48,49</sup> Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to \$50.00 a year.<sup>50</sup>

130. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

131. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

132. The fraudulent activity resulting from the Data Breach may not come to light for years.

133. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

---

<sup>48</sup> <https://www.latimes.com/business/story/2019-11-05/column-data-brokers> (last visited May 6, 2025).

<sup>49</sup> <https://datacoup.com/> (last visited May 6, 2025).

<sup>50</sup> <https://digi.me/what-is-digime/> (last visited May 6, 2025).

134. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to, upon information and belief, thousands to tens of thousands of individuals' detailed personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

135. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

***Future Costs of Credit and Identity Theft Monitoring are Reasonable and Necessary.***

136. Given the type of targeted attack, the sophisticated criminal activity, and the type of Private Information involved in this case, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes –e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims.

137. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her Private Information was used to file for unemployment benefits until law enforcement notifies the individual's employee-benefit management company of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

138. Consequently, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future.

139. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach.

***Loss of Benefit of the Bargain.***

140. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to provide Defendant with their Private Information as a condition of employment and/or enrollment, Plaintiffs and other reasonable employees and students understood and expected that Defendant would properly safeguard and protect their Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

***Plaintiff Lane's Experience***

141. Plaintiff Matthew Lane is a former employee of Defendant.

142. Upon information and belief, as a condition of employment, Plaintiff Lane was required to provide Albion College with his Private Information.

143. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Lane's Private Information in its system.

144. Plaintiff Lane is very careful about sharing his sensitive Private Information. Plaintiff Lane stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

145. Plaintiff Lane provided his Private Information to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

146. Plaintiff Lane reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of Private Information.

147. Plaintiff Lane received the Notice Letter, by U.S. mail, directly from Defendant, dated May 1, 2025. According to the Notice Letter, Plaintiff Lane's Private Information was improperly accessed and obtained by unauthorized third parties, including his name, Social Security number, and bank account information.

148. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructs Plaintiff Lane to monitor his free credit report for any authorized activity, Plaintiff Lane made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect.

149. In fact, Plaintiff Lane has suffered actual injury in the form of fraud. Specifically, Mr. Lane was notified by his financial institution of unauthorized activity on his account. Mr. Lane discovered that an unauthorized individual made multiple purchases using Mr. Lane's bank card.

150. Additionally, Plaintiff Lane has experienced a serious uptick in spam texts and phone calls since the exposure of his Private Information in the Data Breach.

151. These instances of fraud caused Plaintiff Lane to spend significant time on mitigation activities in response to the Data Breach, including but not limited to speaking with

representatives at his bank in attempts to recover his funds, and blocking all numbers that he has received spam texts and calls from.

152. As a result of the Data Breach, Plaintiff Lane spent valuable time that he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

153. Subsequent to the Data Breach, Plaintiff Lane has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) nominal damages; and (vii) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

154. The Data Breach has caused Plaintiff Lane to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

155. As a result of the Data Breach, Plaintiff Lane anticipates spending additional considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

156. As a result of the Data Breach, Plaintiff Lane is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

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

***Plaintiff Knapp's Experience***

158. Plaintiff Zachary Knapp is a former student of Defendant. Plaintiff received a personalized Data Breach notice explaining that his PII was exposed in Defendant's Data Breach.

159. As a condition of enrolling as a student at Albion, Defendant obtained Plaintiff's PII and used that PII to facilitate its operations.

160. Upon information and belief, at the time of the Data Breach, Defendant retained Plaintiff Knapp's Private Information in its system.

161. Plaintiff Knapp is very careful about sharing his sensitive Private Information. Plaintiff Knapp stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

162. Plaintiff Knapp provided his Private Information to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law.

163. Plaintiff Knapp reasonably understood that a portion of the funds derived from his tuition payments to Albion would be used to pay for adequate cybersecurity and protection of PII.

164. Plaintiff Knapp received the Notice Letter, by U.S. mail, directly from Defendant, on or around May 8, 2025. According to the Notice Letter, Plaintiff Knapp's Private Information was improperly accessed and obtained by unauthorized third parties,

including his full name and Social Security number. However, based on Albion's report to the Attorney General of Texas, additional PII, such as Plaintiff's financial and/or driver's license information, may have also been stolen by Medusa in the Data Breach.

165. As a result of the Data Breach, and at the direction of Defendant's Notice Letter, which instructs Plaintiff Knapp to monitor his free credit report for any authorized activity, Plaintiff Knapp made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to monitoring his financial accounts for any indication of fraudulent activity, which may take years to detect.

166. Plaintiff estimates he has spent approximately 5 hours addressing the Data Breach. This includes time researching the Data Breach, time monitoring his accounts to protect himself from identity theft, and time attempting to sign up for the credit monitoring service offered by Defendant in its Breach Notice. After all, Defendant directed Plaintiff to take those steps in its Breach Notice.

167. Plaintiff has been unable to sign up for the credit monitoring offered in Albion's Data Breach as the link contained in its Breach Notice was inoperable.

168. To the best of his knowledge, Plaintiff has not been the victim of another data breach, except for the Data Breach at issue here.

169. Since the Data Breach, Plaintiff has experienced a dramatic increase in scam and phishing texts and emails purporting to be from the IRS and asking him to follow links related to his tax returns. This suggests that his PII has already been placed in the hands of cybercriminals.

170. On information and belief, Plaintiff's email address and phone number was compromised as a result of the Data Breach, as cybercriminals are able to use an individual's PII that is accessible on the dark web, as Plaintiff's is here, to gather and steal even more information.

171. As a result of the Data Breach, Plaintiff Knapp spent valuable time that he otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

172. Subsequent to the Data Breach, Plaintiff Knapp has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vi) nominal damages; and (vii) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

173. The Data Breach has caused Plaintiff Knapp to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

174. As a result of the Data Breach, Plaintiff Knapp anticipates spending additional considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

175. As a result of the Data Breach, Plaintiff Knapp is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

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

### **CLASS ACTION ALLEGATIONS**

177. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to MCR 3.501.

178. The Class that Plaintiffs seek to represent is defined as follows:

**Nationwide Class:** All individuals residing in the United States whose Private Information was accessed and/or acquired by an unauthorized party as a result of the data breach, including those who received notice of the Data Breach (the "Class").

179. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

180. Plaintiffs reserve the right to amend the definitions of the Class or Subclass or add a Class or Subclass if further information and discovery indicate that the definitions of the Class should be narrowed, expanded, or otherwise modified.

181. The proposed Class meets the criteria for certification under MCR 3.501.

182. Numerosity. The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. Although the precise number of individuals is currently unknown to Plaintiffs and exclusively in the possession of Defendant, upon information and belief, thousands of individuals were impacted. The Class is apparently identifiable within

Defendant's records, and Defendant has already identified these individuals (as evidenced by sending them breach notification letters).

183. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. Among the questions of law and fact common to the Class that predominate over questions which may affect individual Class members, including the following:

- a. Whether and to what extent Defendant had a duty to protect the Private Information of Plaintiffs and Class Members;
- b. Whether Defendant had respective duties not to disclose the Private Information of Plaintiffs and Class Members to unauthorized third parties;
- c. Whether Defendant had respective duties not to use the Private Information of Plaintiffs and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiffs and Class Members;
- e. Whether and when Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their Private Information had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their Private Information had been compromised;
- h. Whether 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;

- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Plaintiffs and Class Members are entitled to actual damages and/or nominal damages as a result of Defendant's wrongful conduct; and,
- k. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

184. Typicality. Plaintiffs' claims are typical of those of the other members of the Class because Plaintiffs, like every other Class Member, were exposed to virtually identical conduct and now suffer from the same violations of the law as each other member of the Class.

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

186. Adequacy. Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiffs seek no relief that is antagonistic or adverse to the Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action and data breach litigation, and Plaintiffs intend to prosecute this action vigorously.

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

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

189. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class

Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

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

191. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

192. Further, Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class- wide basis.

193. Likewise, particular issues under MCR 3.501 are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant failed to timely notify the Plaintiffs and the class of the Data Breach;
- b. Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;
- c. Whether Defendant's security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;
- d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

- e. Whether Defendant failed to take commercially reasonable steps to safeguard its clients' employees' Private Information; and,
- f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

## **CAUSES OF ACTION**

### **COUNT I NEGLIGENCE**

#### **(On Behalf of Plaintiffs and the Class)**

194. Plaintiffs re-allege and incorporate by reference all of the allegations contained in the preceding paragraphs, as if fully set forth herein.

195. Defendant requires its employees and students, including Plaintiffs and Class Members, to submit non-public Private Information in the ordinary course of providing its services.

196. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of its business of soliciting its clients, which solicitations and services affect commerce.

197. Plaintiffs and Class Members entrusted Defendant with their Private Information with the understanding that Defendant would safeguard their information.

198. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed.

199. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable

means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

200. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 USC § 45, which prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

201. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

202. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining employment and/or being enrolled with Defendant.

203. 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 Private Information.

204. Defendant was subject to an “independent duty,” untethered to any contract between Defendant and Plaintiffs or the Class.

205. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former employees' Private Information it was no longer required to retain pursuant to regulations.

206. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and the Class of the Data Breach.

207. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

208. Defendant breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Allowing unauthorized access to Class Members' Private Information;
- d. Failing to detect in a timely manner that Class Members' Private Information had been compromised;
- e. Failing to remove former employees' Private Information it was no longer required to retain pursuant to regulations, and;
- f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

209. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

210. Defendant's violation of Section 5 of the FTC Act constitutes negligence.

211. Plaintiffs and Class Members were within the class of persons the Federal Trade Commission Act was intended to protect and the type of harm that resulted from the Data Breach was the type of harm the statute was intended to guard against.

212. The FTC has pursued enforcement actions against businesses, which, as a result 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 the Class.

213. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

214. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches targeting companies in possession of Private Information.

215. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

216. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and the Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

217. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

218. Plaintiffs and the Class had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

219. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

220. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. See Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

221. Defendant has admitted that the Private Information of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

222. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Class, the Private Information of Plaintiffs and the Class would not have been compromised.

223. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and the Class and the harm, or

risk of imminent harm, suffered by Plaintiffs and the Class. The Private Information of Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

224. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) invasion of their privacy; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

225. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

226. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer the continued risks of exposure of their Private Information, 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 the Private Information in its continued possession.

227. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

228. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and insecure manner.

229. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

**COUNT II**  
**NEGLIGENCE *PER SE***  
**(On Behalf of Plaintiffs and the Class)**

230. Plaintiffs re-allege and incorporate by reference all of the allegations contained in the preceding paragraphs, as if fully set forth herein.

231. Section 5 of the FTC Act, 15 USC § 45, prohibits “unfair . . . practices in or affecting commerce” including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect Private Information. Various FTC publications and orders also form the basis of Defendant's duty.

232. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Private Information and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

233. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

234. Plaintiffs and Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

235. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and Class Members.

236. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered or will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) invasion of privacy; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

237. Plaintiffs and Class Members have been injured and are entitled to damages in an amount to be proven at trial.

**COUNT III**  
**BREACH OF THIRD-PARTY BENEFICIARY CONTRACT**  
**(On Behalf of Plaintiffs and the Class)**

238. Plaintiffs re-allege and incorporate by reference all of the allegations contained in the preceding paragraphs, as if fully set forth herein.

239. Defendant offered to provide employment and/or enrollment to its employees and students, including Plaintiffs and Class members, in exchange for payment.

240. Defendant also required Plaintiffs and the Class members to provide their Private Information as a condition of employment and/or enrollment.

241. In turn, Defendant impliedly promised to protect Plaintiffs' and Class members' Private Information through adequate data security measures, including by virtue of the promises in its privacy policies.<sup>51</sup>

242. Plaintiffs and the Class members accepted Defendant's offer by providing Private Information and/or labor to Defendant in exchange for employment and/or enrollment.

243. Plaintiffs and Class members would not have entrusted their Private Information to Defendant but for the above-described agreement with Defendant.

244. Defendant materially breached its agreement(s) with Plaintiffs and Class members by failing to safeguard such Private Information, violating industry standards necessarily incorporated in the agreement.

245. Plaintiffs and Class members have performed under the relevant agreements, or such performance was waived by the conduct of Defendant.

---

<sup>51</sup> See <https://www.albion.edu/offices/information-technology/support/data-privacy-policy/> ("Albion College ("the College") is committed to maintaining the privacy, integrity, security and availability of confidential information created, received, maintained and/or stored by the College, regardless of form.") (last accessed May 6, 2025)

246. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose on each party a duty of good faith and fair dealing. The 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—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract along with its form.

247. Defendant's conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract.

248. The losses and damages Plaintiffs and Class members sustained as described herein were the direct and proximate result of Defendant's breach of the implied contracts with them, including breach of the implied covenant of good faith and fair dealing.

249. Plaintiffs and the Class were harmed by Defendant's breach of its contracts, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

250. Plaintiffs and Class Members are also entitled to their costs and attorney's fees incurred in this action.

**COUNT IV**  
**UNJUST ENRICHMENT**  
**(On Behalf of Plaintiffs and the Class)**

251. Plaintiffs re-allege and incorporate by reference all of the allegations contained in the preceding paragraphs, as if fully set forth herein.

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

253. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have had their Private Information protected with adequate data security.

254. Defendant knew that Plaintiffs and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendant profited from Plaintiffs' retained data and used Plaintiffs' and Class Members' Private Information for business purposes.

255. Defendant failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their Private Information provided.

256. Defendant acquired the Private Information through inequitable record retention as it failed to investigate and/or disclose the inadequate data security practices previously alleged.

257. If Plaintiffs and Class Members had known that Defendant would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would have entrusted their Private Information to Defendant.

258. Plaintiffs and Class Members have no adequate remedy at law.

259. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result

of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

260. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

261. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) actual misuse of the compromised data consisting of an increase in spam calls, texts, and/or emails; (viii) invasion of privacy; (ix) nominal damages; and (x) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

262. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from Defendant and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Defendant from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

263. Plaintiffs and Class Members may not have an adequate remedy at law against Defendant, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

**COUNT V**  
**BREACH OF FIDUCIARY DUTY**  
**(On Behalf of Plaintiffs and the Class)**

264. Plaintiffs re-allege and incorporate by reference all of the allegations contained in the preceding paragraphs, as if fully set forth herein.

265. Given the relationship between Defendant and Plaintiffs and Class members, where Defendant became guardian of Plaintiffs' and Class members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiffs and Class members, (1) for the safeguarding of Plaintiffs and Class members' Private Information; (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.

266. 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 Private Information.

267. Because of the highly sensitive nature of the Private Information, Plaintiffs and Class members (or their third-party agents) would not have entrusted Defendant, or anyone in Defendant's position, to retain their Private Information had they known the reality of Defendant's inadequate data security practices.

268. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to sufficiently encrypt or otherwise protect Plaintiffs' and Class members' Private Information.

269. 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.

270. 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*).

**COUNT VI**  
**DECLARATORY JUDGMENT**  
**(On Behalf of Plaintiffs and the Class)**

271. Plaintiffs re-allege and incorporate by reference all of the allegations contained in the preceding paragraphs, as if fully set forth herein.

272. This Court may enter judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as those alleged herein, which are tortious, and which violate the terms of the federal and state statutes described above.

273. An actual controversy has arisen in the wake of the Data Breach at issue regarding Defendant's common law and other duties to act reasonably with respect to employing reasonable data security. Plaintiffs allege Defendant's actions in this respect were inadequate and unreasonable and, upon information and belief, remain inadequate and unreasonable. Additionally, Plaintiffs and the Class continue to suffer injury due to the continued and ongoing threat of new or additional fraud against them or on their accounts using the stolen data.

274. This Court should enter a judgment declaring, among other things, the following:
- a. Defendant continues to owe a legal duty to employ reasonable data security to secure the Private Information it possesses, and to notify impacted individuals of

the Data Breach under the common law and Section 5 of the FTC Act;

- b. Defendant continues to breach its duty by failing to employ reasonable measures to secure its customers' personal and financial information; and
- c. Defendant's breach of its legal duty continues to cause harm to Plaintiffs and the Class.

275. The Court should also issue corresponding injunctive relief requiring Defendant to employ adequate security protocols consistent with industry standards to protect its customers' (i.e., Plaintiffs' and the Class's) data.

276. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another breach of Defendant's data systems. If another breach of Defendant's data systems occurs, Plaintiffs and the Class will not have 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 to compensate Plaintiffs and the Class for their out-of-pocket and other damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiffs and the Class, which include monetary damages that are not legally quantifiable or provable.

277. The hardship to Plaintiffs and the Class if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued.

278. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the injuries that would result to Plaintiffs, the Class, and the public at large.

#### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, request

judgment against Defendant and that the Court grants the following:

- A. For an order certifying the Class, as defined herein, and appointing Plaintiffs and their Counsel to represent the Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the Private Information of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;
- C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:
  - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
  - ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws.
  - iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;
  - iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;

- v. prohibiting Defendant from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;
- Vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- x. requiring Defendant to conduct regular database scanning and securing checks;
- xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of

Plaintiffs and Class Members;

- xii. requiring Defendant to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. requiring Defendant to implement a system of tests to assess its clients' employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
- xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential Private Information to third parties, as well as the steps affected individuals must take to protect themselves;
- xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate

Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

- D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;
- E. For an award of attorneys' fees and costs as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

Plaintiffs, individually and on behalf of the Class, hereby demand a trial by jury on all claims so triable.

Dated: July 1, 2025

Respectfully submitted,



David H. Fink (P28235)  
Nathan J. Fink (P75185)  
FINK BRESSACK  
38500 Woodward Ave, Suite 350  
Bloomfield Hills, MI 48304  
Telephone: (248) 971-2500  
dfink@finkbressack.com  
nfink@finkbressack.com

Leanna Loginov\*  
SHAMIS & GENTILE P.A.  
14 NE 1st Ave., Suite 705  
Miami, Florida 33132  
Telephone: (305) 479-2299  
lloginov@shamisgentile.com

Raina C. Borrelli\*  
STRAUSS BORRELLI PLLC  
980 N. Michigan Avenue, Suite 1610  
Chicago, Illinois 60611  
Telephone: (872) 263-1100  
raina@straussborrelli.com

*Counsel for Plaintiffs and the Proposed  
Class*

*\*Application for pro hac forthcoming*