UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS

COURTNEY PUGH, individually and on behalf of all others similarly situated,	**Case No.**
Plaintiff,	**CLASS ACTION**
NELSON UNIVERSITY,	**JURY DEMAND**
Defendant.	

CLASS ACTION COMPLAINT

Plaintiff Courtney Pugh ("Plaintiff"), by and through undersigned counsel, on behalf of herself and all others similarly situated, alleges the following Class Action Complaint (the "Action") against Defendant Nelson University ("Defendant") upon personal knowledge as to herself and her own actions, and upon information and belief, including the investigation of counsel as follows:

I. SUMMARY

1. Plaintiff brings this Action on behalf of herself and all other similarly situated victims as a result of a recent cyberattack and data breach involving personally identifiable information and personal health information (collectively "Private Information") suffered by Defendant, which Defendant detected on or about April 6, 2025 (the "Data Breach").

2. Defendant is a private, Christian university in Waxahachie, Texas.[1]

[1] https://www.nelson.edu/about/ (last visited July 31, 2026).

3. Plaintiff and individuals impacted by the Data Breach (the "Class" and the "Class Members") provided their Private Information to Defendant in connection with the education services Defendant provides.

4. On or about April 6, 2025, Defendant became aware that certain systems on its network environment were affected by a data breach, and subsequently launched an investigation into the matter. [2]

5. On June 15, 2026, Defendant began sending notice letters to Plaintiff and Class Members, informing them that their Private Information was exfiltrated in the Data Breach ("Notice").[3]

6. The following types of Private Information were compromised as a result of the Data Breach: names, Social Security numbers, and individual taxpayer identification numbers.[4]

7. Defendant failed to adequately protect Plaintiff's 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 individuals' sensitive data. Hackers targeted and obtained Plaintiff's and Class Members' Private Information because of its value in exploiting and stealing the identities of Plaintiff and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

8. As a result of Defendant's inadequate security and breach of its duties and obligations, the Data Breach occurred, and Plaintiff's and Class Members' Private Information was accessed and disclosed. This action seeks to remedy these failings and their consequences.

[2] See Defendant's notice letter, attached hereto as **Exhibit A**.
[3] *Id.*
[4] *Id.*

Plaintiff brings this action on behalf of herself and all persons whose Private Information was exposed as a result of the Data Breach.

9. Upon information and belief, Plaintiff's Private Information is available on the dark web as a result of the Data Breach.

10. Plaintiff brings 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 Plaintiff and Class Members; (ii) warn Plaintiff 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.

11. Defendant disregarded the rights of Plaintiff and Class Members by (a) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (b) failing to disclose that it did not have adequately robust security protocols and training practices in place to safeguard Plaintiff's and Class Members' Private Information; (c) failing to take standard and reasonably available steps to prevent the Data Breach; (d) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (e) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

12. Plaintiff 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) statutory damages; (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.

13. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

14. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct and asserting claims for: (i) negligence and negligence *per se*, (ii) breach of implied contract, and (iii) unjust enrichment.

15. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, as well as long-term and adequate credit monitoring services funded by Defendant, and declaratory relief.

II. JURISDICTION AND VENUE

16. This Court has jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. The number of class members is more than 100 and at least one member of the Class defined below is a citizen of a different state that is diverse from Defendant's citizenship[5]. Thus, minimal diversity exists under 28 U.S.C. § 1332 (d) (2) (A).

[5] Defendant reported the Data Breach to multiple states' attorney generals, including California, Indiana, Massachusetts, and Vermont. At least 9 Vermont residents and 295 Indiana residents were victims of the Data Breach. *See https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/files/DB-Year-to-Date-*

17. This Court has general personal jurisdiction over Defendant because Defendant maintains its principal places of business in Texas, regularly conduct business in Texas, and enters into contracts within the state of Texas.

18. Venue is proper in this Court because Defendant's principal place of business is located in this District, and because a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

III. PARTIES

Plaintiff

19. Plaintiff is an individual citizen and resident of Oak Leaf, Texas.

Defendant

20. Defendant is a private university in the State of Texas, maintaining its principal place of business at 1200 Sycamore St., Waxahachie, Texas 75165.

IV. FACTUAL ALLEGATIONS

Defendant's Business

21. Defendant is a private, Christian university in Waxahachie, Texas.[6]

22. Defendant collects personally identifiable information in the course of doing business. This personally identifiable information includes the Private Information of Plaintiff and Class Members which was compromised in the Data Breach alleged herein. But for Defendant's collection of Plaintiff's and Class Members' Private Information, Defendant would be unable to provide its services.

Report-7_2026.pdf; https://ago.vermont.gov/categories/security-breach-notices; https://oag.ca.gov/ecrime/databreach/reports/sb24-624948.

[6] https://www.nelson.edu/about/ (last visited July 31, 2026).

23. Upon information and belief, Defendant promises to maintain the confidentiality of Plaintiff's and Class Members' Private Information to ensure compliance with federal and state laws and regulations, and not to use or disclose Plaintiff's and Class Members' Private Information for non-essential purposes.

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

25. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class Members would not have entrusted Defendant with their Private Information had they known that Defendant would fail to implement industry standard protections for that sensitive information.

26. Plaintiff and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

27. Defendant assumed sole and exclusive control over its data security. Once Plaintiff and Class Members provided their Private Information to Defendant, Defendant was in the exclusive position to protect and safeguard the Private Information.

The Attack and Data Breach

28. On June 15, 2026, Defendant began sending notice letters ("Notice") to affected individuals, informing them of the Data Breach. [7] The Notice states:

What Happened?

[7] Ex. A.

> On or about April 6, 2025, our IT team became aware of potential unauthorized access on our network. Upon learning of this issue, we took steps to ensure the security of our systems and we commenced a prompt and thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals experienced in handling these types of situations to assist us in determining the full extent of the incident and the scope of any data impacted. Our investigation revealed that an unauthorized actor accessed our systems from on or about March 21, 2025, to on or about April 6, 2025, and, as a result, possibly viewed and/or obtained certain files from our network. On or about May 26, 2026, after an extensive forensic investigation and manual document review, we discovered your personal information was included within the impacted data.
>
> *What Information Was Involved*
>
> The impacted files contained your full name and Social Security number or individual taxpayer identification number.[8]

29. To be clear, there are numerous issues with Defendant's Data Breach, but the deficiencies in the Data Breach Notice exacerbate the circumstances for victims of the Data Breach: (1) Defendant fails to state whether it was able to contain or end the cybersecurity threat, leaving victims to fear whether the Private Information that Defendant continues to maintain is secure; (2) Defendant fails to state how the Breach itself occurred; (3) Defendant's data security measures are so insufficient that Defendant did not detect the Data Breach until the unauthorized access had occurred for more than ***two weeks***; and (4) Defendant waited over ***a full year*** after learning of the Data Breach to notify affected individuals, depriving victims of the earliest opportunity to take preventative measures to protect their Private Information. All of this information is vital to victims of a data breach, let alone a data breach of this magnitude due to the sensitivity of information compromised in this specific breach.

30. Despite Defendant's intentional opacity about the root cause of this incident, several facts may be gleaned from the Notice, including: a) that this Data Breach was the work of

[8] *Id.*

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 Plaintiff's and Class Members' Private Information and other sensitive information for download and theft.

31. Moreover, in its Notice, 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.

32. Furthermore, Defendant's delay in notifying Plaintiff and Class Members of the Data Breach is in direct violation of Defendant's responsibilities under the data breach notification statute in Texas. *See* Tex. Bus. & Com. Code § 521.053(b) which requires that the disclosure notification be "made without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred".

33. Defendant failed to meet this requirement by ***375 days***, as it learned of the Data Breach on or about April 6, 2025, but waited to notify affected individuals until June 15, 2026.

34. Due to Defendant's inadequate security measures, Plaintiff and the Class Members now face a present, immediate, and ongoing risk of fraud and identity theft and must deal with that threat forever.

35. Upon information and belief, the Private Information was not encrypted or redacted prior to the Data Breach.

36. Upon information and belief, the cyberattack was targeted at Defendant as a company that collects and maintains valuable personal data from its many applicants, students, employees, and other individuals interested in receiving Defendant's services, including Plaintiff and Class Members.

37. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the Private Information of Plaintiff and Class Members.

38. Defendant had obligations to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

39. Plaintiff 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.

40. Upon information and belief, Defendant made promises to Plaintiff and Class Members to maintain and protect their Private Information, demonstrating an understanding of the importance of securing Private Information.

41. Acknowledging the harm that the Data Breach presents, Defendant offered victims one year of complimentary credit monitoring services – an offer that is inadequate considering that victims of the Data Breach will likely suffer an increased risk of identity theft and other harms for years into the future, if not for their respective lifetimes.[9]

The Data Breach Was Foreseeable and the Defendant Was Aware of Its Risk

42. It is well known that Private Information, including Social Security numbers in particular, is an invaluable commodity and a frequent target of hackers.

[9] *Id.*

43. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting institutions that collect and store Private Information, like Defendant, preceding the date of the Data Breach.

44. In 2023, a record 3,205 data breaches occurred in the United States, resulting in about 349,221,481 sensitive records being exposed, a greater than 100% increase from 2019.[10] These statistics have held steady for 2024 – when 3,158 data compromises occurred. [11]

45. Individuals place a high value not only on their Private Information, but also on the privacy of that data. For the individual, identity theft causes significant negative financial impact on victims as well as severe distress and other strong emotions and physical reactions.

46. 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), LoanDepot (16.9 million affected, January 2024), Evolve Bank & Trust (7.6 million affected, May 2024), Financial Business and Consumer Solutions (4.2 million affected, February 2024), and Prudential Financial (2.5 million affected, February 2024), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

47. Indeed, cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of and take appropriate measures to prepare for and are able to thwart such an attack.

[10] [10] ITRC (Identity Theft Resource Center), *2023 Data Breach Report* (January 2024), *available at* https://www.idtheftcenter.org/post/2023-annual-data-breach-report-reveals-record-number-of-compromises-72-percent-increase-over-previous-high/ (last visited July 31, 2026).
[11] [11] ITRC (Identity Theft Resource Center), *2024 Data Breach Report* (January 2025), *available at* https://www.idtheftcenter.org/publication/2024-data-breach-report/ (last visited July 31, 2026).

48. Additionally, as companies became more dependent on computer systems to run their business, *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.

49. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff 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 Plaintiff and Class Members as a result of a breach.

50. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

51. Despite the prevalence of public announcements of data breach and data security compromises, and despite its own acknowledgment of its duties to keep the Private Information private and secure, Defendant failed to take appropriate steps to protect the Private Information of Plaintiff and the proposed Class from being compromised.

Defendant Could Have Prevented the Data Breach

52. Data breaches are preventable.[12] "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[13] "Organizations that collect, use, store, and share sensitive

[12] Lucy L. Thomson, *Despite the Alarming Trends, Data Breaches Are Preventable*, DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012), available at https://lawcat.berkeley.edu/record/394088.
[13] *Id.* at 17.

personal data must accept responsibility for protecting the information and ensuring that it is not compromised[.]"[14]

53. Most reported data breaches "are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[15]

54. Here, many failures laid the groundwork for the Data Breach.

55. The Federal Trade Commission ("FTC") has published guidelines that establish reasonable data security practices for businesses.[16]

56. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[17]

57. The FTC guidelines establish that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems.[18]

58. The FTC guidelines also recommend that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[19]

---

[14] *Id.* at 28.
[15] *Id.*
[16] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[17] *Id.*
[18] *Id.*
[19] *Id.*

59. According to information and belief, Defendant failed to follow reasonable and necessary industry standards to prevent a data breach, including the FTC's guidelines.

60. Defendant was at all times fully aware of its obligation to protect the Private Information of consumers under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), yet failed to comply with such obligations. 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 Plaintiff and the Class.

61. Based on allowing its security certificates to lapse and upon information and belief, Defendant also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in cybersecurity readiness.

62. 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."[20]

63. To prevent and detect the attack here, Defendant could and should have taken, as recommended by the Federal Bureau of Investigation, the following measures:

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

- Implemented 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.
- Enabled 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.
- Scanned all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configured firewalls to block access to known malicious IP addresses.
- Patched 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.
- Managed 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.
- Configured 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.

- Disabled 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.
- Implemented 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.
- Considered disabling Remote Desktop protocol (RDP) if it is not being used.
- Used application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Executed operating system environments or specific programs in a virtualized environment.
- Categorized data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[21]

64. According to information and belief, Defendant failed to do any of the above.

65. To prevent and detect cyberattacks, Defendant could and should have recommended its employees take, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

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

[21] *Id.* at 3–4.

- **Used caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net).
- **Opened email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Kept your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it.
- **Verified email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you

when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Used and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.[22]

66. In addition, to prevent and detect the Data Breach Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

- **Harden internet-facing assets**
  - Apply latest security updates
  - Use threat and vulnerability management
  - Perform regular audits
- **Thoroughly investigate and remediate alerts.**
  - Prioritize and treat commodity malware infections as potential full compromise of the system
- **Include IT professionals in security discussions.**
  - Ensure collaboration among security operations, security administrators, and information technology administrators to configure servers and other endpoints securely
- **Build and maintain credential hygiene**

[22] *See Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (revised Sept. 2, 2021), https://www.cisa.gov/news-events/news/protecting-against-ransomware (internal citations omitted).

- Use multifactor authentication or network level authentication and enforce strong, randomized, just-in-time local administrator 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**
  - Utilize 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[23]

67. Specifically, among other failures, Defendant had far too much confidential unencrypted information held on its systems. Such Private Information should have been segregated into an encrypted system.[24]

68. Moreover, it is well-established industry standard practice for a business to dispose of confidential Private Information once it is no longer needed.[25]

[23] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT THREAT INTELLIGENCE (Mar 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.
[24] *See* Adnan Raja, *How to Safeguard Your Business Data With Encryption*, DATAINSIDER (Aug. 14, 2018), https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption.
[25] *See Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.

69. The FTC has repeatedly emphasized the importance of disposing of unnecessary Private Information: "Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it's not on your system, it can't be stolen by hackers."[26] Rather than following this basic standard of care, Defendant kept thousands of individuals' unencrypted Private Information on its inadequately secured systems indefinitely.

70. In sum, the Data Breach could have been easily prevented through standard practices like the use of industry standard network segmentation, redaction, and encryption of all Private Information—which Defendant negligently failed to do.

71. Further, the scope of the Data Breach could have been dramatically reduced had Defendant utilized proper record retention and destruction practices—but Defendant negligently did no such thing.

Defendant Had a Duty to Plaintiff and Class Members to Secure Private Information

72. At all relevant times, Defendant had a duty to Plaintiff and Class Members to properly secure their Private Information, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiff and Class Members, and to *promptly* notify Plaintiff and Class Members when Defendant became aware that their Private Information may have been compromised.

73. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiff and the Class Members, on the other hand. The special relationship arose because Plaintiff and the Members of the Class

[26] *Id.* at 6.

relied on Defendant to secure their Private Information when they entrusted Defendant with the information required in connection with the services Defendant provides.

74. Once Plaintiff and Class Members provided their Private Information to Defendant, Defendant was in the exclusive position to protect and safeguard the Private Information.

75. Defendant had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Defendant breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

76. Security standards commonly accepted among businesses that store Private Information using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for Private Information;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

77. The ramifications of Defendant's failure to keep Private Information secure are long lasting and severe. Once Private Information is stolen, particularly Social Security numbers,

fraudulent use of that information and damage to victims is likely to continue for years.

The Value of Personally Identifiable Information

78. The Private Information of consumers 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. For example, personal information can be sold at a price ranging from $40 to $200, [27] and bank details can have a price range of $30 to over $4,000.[28]

79. As a growing number of federal courts have begun to recognize the loss of value of Private Information as a viable damages theory, the sale of Private Information from data breaches, as in the Data Breach alleged herein, is particularly harmful to data breach victims – especially when it takes place on the dark web.

80. The dark net is an unindexed layer of the internet that requires special software or authentication to access.[29] Criminals in particular favor the dark web as it offers a degree of anonymity to visitors and website publishers. Unlike the traditional or 'surface' web, dark web users need to know the web address of the website they wish to visit in advance. For example, on the surface web, the CIA's web address is cia.gov, but on the dark web the CIA's web address is ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion.[30] This prevents dark web marketplaces from being easily identifiable to authorities or those not in the know.

81. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, sensitive personal information like the Private

[27] *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 July 31, 2026).
[28] https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited July 31, 2026).
[29] *What Is the Dark Web?,* Experian, *available at* https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last visited July 31, 2026).
[30] *Id*.

Information at issue here.[31] The digital character of Private Information stolen in data breaches lends itself to dark web transactions because it is immediately transmissible over the internet and the buyer and seller can retain their anonymity. The sale of a firearm or drugs on the other hand requires a physical delivery address. Nefarious actors can readily purchase usernames and passwords for online streaming services, stolen financial information and account login credentials, and Social Security numbers, dates of birth and other personal information.[32] As Microsoft warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others." [33]

82. Plaintiff's and Class Members' Private Information is a valuable commodity, a market exists for Plaintiff's and Class Members' Private Information (which is why the Data Breach was perpetrated in the first place), and Plaintiff's and Class Members' Private Information is likely being sold by hackers on the dark web (as that is the *modus operandi* of data thieves). As a result, Plaintiff and Class Members have lost the value of their Private Information, which is sufficient to plausibly allege injury arising from a data breach.

83. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[34] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[35]

[31] *What is the Dark Web?* – Microsoft 365, *available at* https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web (last visited July 31, 2026).
[32] *Id.*; *What Is the Dark Web?,* Experian, *available at* https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (last visited July 31, 2026).
[33] *What is the Dark Web?* – Microsoft 365, *available at* https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/what-is-the-dark-web (last visited July 31, 2026).
[34] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited July 31, 2026).
[35] https://datacoup.com/ (last visited July 31, 2026).

Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $60.00 a year.[36]

84. The Private Information stolen in this specific Data Breach was particularly harmful, as it is difficult, if not impossible to change names, dates of birth, and Social Security numbers.

85. Of course, a stolen Social Security number – standing alone – can be used to wreak untold havoc upon a victim's personal and financial life. The popular personal privacy and credit monitoring service LifeLock by Norton notes "Five Malicious Ways a Thief Can Use Your Social Security Number," including: 1) Financial Identity Theft that includes "false applications for loans, credit cards or bank accounts in your name or withdraw money from your accounts," and which can encompass credit card fraud, bank fraud, computer fraud, wire fraud, mail fraud and employment fraud; 2) Government Identity Theft, including tax refund fraud; 3) Criminal Identity Theft, which involves using someone's stolen Social Security number as a "get out of jail free card;" 4) Medical Identity Theft; and 5) Utility Fraud.

86. It is little wonder that courts have dubbed a stolen Social Security number as the "gold standard" for identity theft and fraud. Social Security numbers, which were compromised in the Data Breach, are among the worst kinds of private information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

87. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information

[36] Nielsen Computer & Mobile Panel, Frequently Asked Questions, available at https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited July 31, 2026).

increases." [37] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[38]

88. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, when they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[39]

89. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[40] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[41]

90. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

---

[37] *See* https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases. (last visited July 31, 2026)
[38] *Id.*
[39] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 31, 2026)
[40] *See* https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/ (last visited July 31, 2026)
[41] *See* https://www.investopedia.com/terms/s/ssn.asp (last visited July 31, 2026)

91. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[42]

92. For these reasons, some courts have referred to Social Security numbers as the "gold standard" for identity theft. *Portier v. NEO Tech. Sols*., No. 3:17-CV-30111, 2019 WL 7946103, at *12 (D. Mass. Dec. 31, 2019) ("Because Social Security numbers are the gold standard for identity theft, their theft is significant . . . . Access to Social Security numbers causes long-lasting jeopardy because the Social Security Administration does not normally replace Social Security numbers."), report and recommendation adopted, No. 3:17-CV-30111, 2020 WL 877035 (D. Mass. Jan. 30, 2020); *see also McFarlane v. Altice USA, Inc*., 2021 WL 860584, at *4 (citations omitted) (S.D.N.Y. Mar. 8, 2021) (the court noted that Plaintiff's Social Security numbers are: arguably "the most dangerous type of personal information in the hands of identity thieves" because it is immutable and can be used to "impersonat[e] [the victim] to get medical services, government benefits, ... tax refunds, [and] employment." . . . Unlike a credit card number, which can be changed to eliminate the risk of harm following a data breach, "[a] social security number derives its value in that it is immutable," and when it is stolen it can "forever be wielded to identify [the victim] and target him in fraudulent schemes and identity theft attacks.")

93. Private Information can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an

[42] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last visited July 31, 2026).

individual, such as their birthdate, birthplace, and mother's maiden name.[43]

94. Given the nature of Defendant's Data Breach, as well as the unreasonable delay in notification to Class Members, it is foreseeable that the compromised Private Information has been or will be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' Private Information can easily obtain Plaintiff's and Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

95. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures.

The Harm Caused by the Data Breach Now and Going Forward

96. Victims of data breaches are susceptible to becoming victims of identity theft for years to come. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 17 C.F.R. § 248.201(9).

97. The type of data that may have been accessed and compromised here can be used to perpetrate fraud and identity theft and Plaintiff and Class Members face a substantial risk of identity theft given that their Private Information was compromised in the Data Breach.

98. When malicious actors infiltrate companies and copy and exfiltrate the Private Information that those companies store, the stolen information often ends up on the dark web, where malicious actors buy and sell that information for profit.[44]

99. For example, when the U.S. Department of Justice announced their seizure of AlphaBay—the largest online "dark market"—in 2017, AlphaBay had more than 350,000 listings,

[43] *See* OFFICE OF MGMT. & BUDGET, OMB MEMORANDUM M-07-16 n. 1.
[44] *Shining a Light on the Dark Web with Identity Monitoring*, IDENTITYFORCE (Dec. 28, 2020) https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited July 31, 2026).

many of which concerned stolen or fraudulent documents that could be used to assume another person's identity.[45] Marketplaces similar to the now-defunct AlphaBay continue to be "awash with [Private Information] belonging to victims from countries all over the world."[46]

100. 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.

101. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity—or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

102. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches can be the starting point for these additional targeted attacks on the victim.

103. One such example of criminals piecing together bits and pieces of compromised

[45] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, ARMOR (April 3, 2018) https://res.armor.com/resources/blog/stolen-pii-ramifications-identity-theft-fraud-dark-web/ (last visited July 31, 2026).
[46] *Id.*

Private Information for profit is the development of "Fullz" packages.[47]

104. 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.

105. 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 Plaintiff's 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 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.

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

106. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good."[48] Defendant did not rapidly report to Plaintiff and Class Members that

[47] "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 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://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/.(last visited July 31, 2026).

[48] *2019 Internet Crime Report Released*, FBI (Feb. 11, 2020) https://www.fbi.gov/news/stories/2019-internet-crime-report-released-

their Private Information had been stolen. Defendant did not notify impacted people for over fourteen months after learning of the Data Breach.

107. 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.

108. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience as a result of the Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts for any indication of fraudulent activity, which may take years to detect.

109. These efforts are consistent with the U.S. Government Accountability Office, which 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."[49]

110. These efforts are also consistent with the steps that FTC recommends that data breach victims take to protect their personal and financial information after a data breach,

021120#:~:text=IC3%20received%20467%2C361%20complaints%20in,%2Ddelivery%20scams%2C%20and%20extortion (last visited July 31, 2026).

[49] *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 July 31, 2026).

including: contacting one of the credit bureaus to place a fraud alert (and considering an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[50]

Diminution of Value of Private Information

111. Private Information is a valuable property right.[51] The 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 a doubt that Private Information has considerable market value.

112. As a result of the Data Breach, Plaintiff's 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 Plaintiff 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.

113. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff 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 Plaintiff and Class Members as a result of a breach.

---

[50] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps. (last visited July 31, 2026).

[51] *See, e.g.*, Randall 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 July 31, 2026).

114. As a result of the Data Breach, the Private Information of Plaintiff and Class Members has been exposed to criminals for misuse. The injuries suffered by Plaintiff and Class Members, or likely to be suffered as a direct result of Defendant's Data Breach, include: (a) theft of their Private Information; (b) costs associated with the detection and prevention of identity theft; (c) costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the consequences of this Breach; (d) invasion of privacy; (e) the emotional distress, stress, nuisance, and annoyance of responding to, and resulting from, the Data Breach; (f) the actual and/or imminent injury arising from actual and/or potential fraud and identity theft resulting from their personal data being placed in the hands of the ill-intentioned hackers and/or criminals; (g) damage to and diminution in value of their personal data entrusted to Defendant with the mutual understanding that Defendant would safeguard their Private Information against theft and not allow access to and misuse of their personal data by any unauthorized third party; and (h) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further injurious breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

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

116. Given the type of targeted attack in this case and sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breach, 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.

117. Such fraud may go undetected for years; consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

118. As a result, Plaintiff and Class Members also request relief in the form of the future cost of credit and identity theft monitoring, which is reasonable and necessary. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft that arose from the Data Breach.

Loss of the Benefit of the Bargain

119. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to provide their Private Information to Defendant, Plaintiff and other reasonable applicants, students, employees, and individuals interested in receiving Defendant's services, understood and expected that in exchange, Defendant would implement necessary data security to protect the Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

Plaintiff's Experience

120. Plaintiff is a former student of Defendant, and provided her Private Information to Defendant as a condition of enrollment with Defendant.

121. On or around June 15, 2026, Plaintiff received Defendant's Notice informing her that her Private Information was exposed in the Data Breach.[52] Plaintiff is a victim of the Data Breach.

122. To date, Defendant has done next to nothing to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this Data Breach particularly given the fact that Plaintiff's Private Information has already been "impacted" in the Data Breach and likely been made available on the dark web to anyone wishing to purchase it.

123. Nor has Defendant compensated Plaintiff and Class Members for the time they will spend monitoring their accounts, placing credit freezes and fraud alerts, changing online passwords and other actions.

124. Plaintiff and Class Members have been further damaged by the compromise of their Private Information in the Data Breach which was "impacted" and is in the hands of cybercriminals who illegally accessed Defendant's network for the specific purpose of targeting the Private Information.

125. Plaintiff typically takes measures to protect her Private Information and is very careful about sharing her Private Information. Plaintiff has never knowingly transmitted unencrypted Private Information over the internet or other unsecured source.

126. Plaintiff stores any documents containing her Private Information in a safe and secure location, and she diligently chooses unique usernames and passwords for her online accounts.

127. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. In

[52] Ex. A.

response to the Data Breach, Plaintiff has spent time monitoring her accounts and credit score, changing her online account passwords, freezing her bank accounts, enrolling in credit monitoring, verifying the legitimacy of the Data Breach, and on other necessary mitigation efforts. This is time that was lost and unproductive and took away from other activities and duties.

128. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of her Private Information — a form of intangible property that she entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and as a result of the Data Breach.

129. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

130. Plaintiff suffered emotional distress and increased stress and anxiety as a result of the Data Breach because of the actions she has been forced to undertake, the loss of control over her most intimate information, and the fact that she must remain vigilant for the remainder of her life.

131. Plaintiff has suffered imminent and impending injury arising from the increased risk of fraud, identity theft, and misuse resulting from her Private Information being placed in the hands of criminals.

132. Further, since the Data Breach occurred, Plaintiff has experienced actual misuse of her Private Information; for example, an unauthorized individual attempted to open an Amazon account and other accounts using her Private Information. Because of the timing of the suspicious activities that Plaintiff has experienced and the Data Breach, Plaintiff believes that the suspicious activities are a result of criminals acquiring her Private Information in the Data Breach.

133. Defendant obtained and continues to maintain Plaintiff's Private Information and

has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Defendant acquired Plaintiff's Private Information. Plaintiff, however, would not have entrusted her Private Information to Defendant had she known that it would fail to maintain adequate data security. Plaintiff's Private Information was compromised and disclosed as a result of the Data Breach.

134. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

V. CLASS ACTION ALLEGATIONS

135. Plaintiff brings this class action pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following class:

> All persons whose Private Information was compromised as a result of the Data Breach, including all persons who received Defendant's Notice (the "Class").

136. 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 has 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.

137. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, approximately 37,313 individuals have been affected

by this breach[53]. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

138. **Commonality.** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

i. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

ii. 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;

iii. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

iv. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

v. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

vi. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

vii. Whether computer hackers obtained Class Members' Private Information in the Data Breach;

viii. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

[53]https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/files/DB-Year-to-Date-Report-7_2026.pdf

ix. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

x. Whether Defendant's conduct was negligent; and

xi. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

139. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

140. **Adequacy of Representation.** Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating Class actions, including data privacy litigation of this kind.

141. **Predominance.** Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

142. **Superiority.** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to

individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

143. 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.

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

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

xiii. Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

xiv. Whether Defendant's failure to institute adequate protective security measures amounted to negligence; and

xv. Whether Defendant failed to take commercially reasonable steps to safeguard Private Information.

145. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

VI. CAUSES OF ACTION

COUNT I
NEGLIGENCE/NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

146. Plaintiff hereby repeats and realleges paragraphs 1 through 145 of this Complaint and incorporates them by reference herein.

147. Defendant knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information for pecuniary gain, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties.

148. Defendant had a duty under common law to have procedures in place to detect and prevent the loss or unauthorized dissemination of Plaintiff's and Class Members' Private Information.

149. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information were wrongfully disclosed. The harm that Plaintiff and Class Members experienced was within the zone of foreseeable harm known to Defendant.

150. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class directly or indirectly entrusted Defendant with their confidential Private Information, a mandatory step in obtaining services from Defendant. While this special relationship exists independent from any contract, it is recognized by Defendant's representations, as well as applicable laws and regulations. Specifically, Defendant actively solicited and gathered Private Information as part of its business and was solely responsible for

and in the position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a resulting data breach.

151. Once Plaintiff and Class Members provided their Private Information to Defendant, Defendant was in the exclusive position to protect and safeguard the Private Information.

152. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff and the Class, to maintain adequate data security.

153. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices and the frequency of data breaches in general.

154. Defendant also had a common law duty to prevent foreseeable harm to others. Plaintiff and the Class were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiff and the Class, the critical importance of adequately safeguarding that Private Information, and the necessity of encrypting Private Information stored on Defendant's systems. It was foreseeable that Plaintiff and Class Members would be harmed by the failure to protect their personal information because hackers are known to routinely attempt to steal such information and use it for nefarious purposes.

155. Defendant's conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's wrongful conduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with industry standards for the safekeeping of Plaintiff's and the Class's Private Information, including basic encryption techniques available to Defendant.

156. Plaintiff and the Class had and have no ability to protect their Private Information that was in, and remains in, Defendant's possession.

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

158. 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 safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

159. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within Defendant's possession.

160. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiff's and Class Members' Private Information.

161. Defendant, through its actions and/or omissions, unlawfully breached its duty to timely disclose to Plaintiff and Class Members that the Private Information within Defendant's possession might have been compromised and precisely the type of information compromised.

162. Defendant's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised.

163. Pursuant to Section 5 of the FTCA, Defendant had a separate and independent duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

164. The FTCA is intended, in part, to protect individuals whose Private Information is maintained by another and who are unable to safeguard their information as they cannot exercise control or direction over the data security practices.

165. Plaintiff and the members of the Class are within the class of persons that the FTCA was intended to protect as their Private Information was collected and maintained by Defendant and they were unable to exercise control over Defendant's data security practices.

166. The harm that occurred as a result of the Data Breach is the type of harm the FTCA was intended to guard against.

167. 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 Plaintiff and the members of the Class.

168. Defendant breached its duties to Plaintiff and the members of the Class under the Federal Trade Commission Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

169. Had Plaintiff and the members of the Class known that Defendant would not adequately protect their Private Information, Plaintiff and the members of the Class would not have entrusted Defendant with their Private Information.

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

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

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

173. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information for Plaintiff's and Class Members' respective lifetimes; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and other identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remains 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; and (viii) present and future costs in the form of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the compromise of Private Information as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class Members.

174. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff 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.

175. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remains 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.

176. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class are now at an increased risk of identity theft or fraud.

177. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff is entitled to and demands actual, consequential, and nominal damages and injunctive relief to be determined at trial.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

178. Plaintiff hereby repeats and realleges paragraphs 1 through 145 of this Complaint and incorporates them by reference herein.

179. Plaintiff and the Class entrusted their Private Information to Defendant in connection with the services Defendant provides. In so doing, Plaintiff and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

180. At the time Defendant acquired the Private Information of Plaintiff and the Class, there was a meeting of the minds and a mutual understanding that Defendant would safeguard the Private Information and not take unjustified risks when storing the Private Information.

181. Implicit in the agreements between Plaintiff and Class Members and Defendant to provide Private Information was the latter's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the Private Information only under conditions that kept such information secure and confidential.

182. Plaintiff and the Class would not have entrusted their Private Information to Defendant had they known that Defendant would make the Private Information internet-accessible, not encrypt sensitive data elements, and not delete the Private Information when Defendant no longer had a reasonable need to maintain it.

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

184. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to provide timely and accurate notice to them that personal information was compromised as a result of the Data Breach.

185. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and

economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

186. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages to be determined at trial.

COUNT III
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

187. Plaintiff hereby repeats and realleges paragraphs 1 through 145 of this Complaint and incorporates them by reference herein.

188. This Count is brought in the alternative to Count II, Breach of Implied Contract.

189. Plaintiff and Class Members conferred a monetary benefit on Defendant by providing Defendant with their valuable Private Information. In so conferring this benefit, Plaintiff and Class Members understood that part of the benefit Defendant derived from the Private Information would be applied to data security efforts to safeguard the Private Information.

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

191. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class

Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

192. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

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

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

195. Plaintiff and Class Members have no adequate remedy at law.

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

prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

198. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that it unjustly received from them.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class defined herein, prays for judgment as against Defendant as follows:

a.) For an Order certifying this action as a Class action and appointing Plaintiff and her 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 Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

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

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

e.) Ordering Defendant to pay for lifetime credit monitoring services for Plaintiff and the Class;

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

g.) For an award of punitive damages, as allowable by law;

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

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

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

JURY TRIAL DEMAND

Plaintiff hereby demands a trial by jury.

DATED: July 31, 2026

Respectfully submitted,

/s/ Leanna Loginov
Leanna A. Loginov
SHAMIS & GENTILE, P.A.
2626 Cole Avenue, Suite 300
Dallas, Texas 75204
Tel: (305) 479-2299
lloginov@shamisgentile.com

Attorneys for Plaintiff and the Class