Supreme Court of Pennsylvania
Court of Common Pleas
Civil Cover Sheet
LUZERNE County

For Prothonotary Use Only:	TIME STAMP
Docket No: 202512631	

The information collected on this form is used solely for court administration purposes. This form does not supplement or replace the filing and service of pleadings or other papers as required by law or rules of court.

SECTION A

Commencement of Action:
☒ Complaint ☐ Writ of Summons ☐ Petition
☐ Transfer from Another Jurisdiction ☐ Declaration of Taking

Lead Plaintiff's Name:	Lead Defendant's Name:
Dean Ambosie, et al.,	Wilkes University,
Are money damages requested? ☒ **Yes** ☐ **No**	Dollar Amount Requested: (check one) ☐ within arbitration limits ☒ outside arbitration limits
Is this a *Class Action Suit*? ☒ **Yes** ☐ **No**	**Is this an *MDJ Appeal*?** ☐ **Yes** ☒ **No**

Name of Plaintiff/Appellant's Attorney: Kenneth J. Grunfeld

☐ **Check here if you have no attorney (are a Self-Represented [Pro Se] Litigant)**

SECTION B

Nature of the Case: Place an "X" to the left of the **ONE** case category that most accurately describes your ***PRIMARY CASE.*** If you are making more than one type of claim, check the one that you consider most important.

TORT *(do not include Mass Tort)*
- ☐ Intentional
- ☐ Malicious Prosecution
- ☐ Motor Vehicle
- ☐ Nuisance
- ☐ Premises Liability
- ☐ Product Liability *(does not include mass tort)*
- ☐ Slander/Libel/ Defamation
- ☒ Other: data breach

MASS TORT
- ☐ Asbestos
- ☐ Tobacco
- ☐ Toxic Tort - DES
- ☐ Toxic Tort - Implant
- ☐ Toxic Waste
- ☐ Other:

PROFESSIONAL LIABLITY
- ☐ Dental
- ☐ Legal
- ☐ Medical
- ☐ Other Professional:

CONTRACT *(do not include Judgments)*
- ☐ Buyer Plaintiff
- ☐ Debt Collection: Credit Card
- ☐ Debt Collection: Other
- ☐ Employment Dispute: Discrimination
- ☐ Employment Dispute: Other
- ☐ Other:

REAL PROPERTY
- ☐ Ejectment
- ☐ Eminent Domain/Condemnation
- ☐ Ground Rent
- ☐ Landlord/Tenant Dispute
- ☐ Mortgage Foreclosure: Residential
- ☐ Mortgage Foreclosure: Commercial
- ☐ Partition
- ☐ Quiet Title
- ☐ Other:

CIVIL APPEALS
Administrative Agencies
- ☐ Board of Assessment
- ☐ Board of Elections
- ☐ Dept. of Transportation
- ☐ Statutory Appeal: Other
- ☐ Zoning Board
- ☐ Other:

MISCELLANEOUS
- ☐ Common Law/Statutory Arbitration
- ☐ Declaratory Judgment
- ☐ Mandamus
- ☐ Non-Domestic Relations Restraining Order
- ☐ Quo Warranto
- ☐ Replevin
- ☐ Other:

Updated 1/1/2011

NOTICE

Pennsylvania Rule of Civil Procedure 205.5. (Cover Sheet) provides, in part:

Rule 205.5. Cover Sheet

(a)(1) This rule shall apply to all actions governed by the rules of civil procedure except the following:

(i) actions pursuant to the Protection from Abuse Act, Rules 1901 et seq.

(ii) actions for support, Rules 1910.1 et seq.

(iii) actions for custody, partial custody and visitation of minor children, Rules 1915.1 et seq.

(iv) actions for divorce or annulment of marriage, Rules 1920.1 et seq.

(v) actions in domestic relations generally, including paternity actions, Rules 1930.1 et seq.

(vi) voluntary mediation in custody actions, Rules 1940.1 et seq.

(2) At the commencement of any action, the party initiating the action shall complete the cover sheet set forth in subdivision (e) and file it with the prothonotary.

(b) The prothonotary shall not accept a filing commencing an action without a completed cover sheet.

(c) The prothonotary shall assist a party appearing pro se in the completion of the form.

(d) A judicial district which has implemented an electronic filing system pursuant to Rule 205.4 and has promulgated those procedures pursuant to Rule 239.9 shall be exempt from the provisions of this rule.

(e) The Court Administrator of Pennsylvania, in conjunction with the Civil Procedural Rules Committee, shall design and publish the cover sheet. The latest version of the form shall be published on the website of the Administrative Office of Pennsylvania Courts at www.pacourts.us.

KOPELOWITZ OSTROW P.A.
KENNETH J. GRUNFELD, ESQUIRE
Identification No.: 84121
65 Overhill Road
Bala Cynwyd, PA 19004
Tel.: (954) 525-4100
grunfeld@kolawyers.com

Attorneys for Plaintiff
(additional counsel listed below)

IN THE COURT OF COMMON PLEAS OF LUZERNE COUNTY, PENNSYLVANIA

DEAN AMBOSIE, JENNA BALSAMELLO, NICHOLE DUDEN, MACKENZIE PAWELZIK, VINCENT ABBOTT, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

WILKES UNIVERSITY,

Defendant.

CLASS ACTION

JURY TRIAL DEMANDED

Case No.: 202512631

NOTICE TO DEFEND

You have been sued in court. If you wish to defend against the claims set forth in the following pages, you must take action within twenty (20) days after this complaint and notice are served, by entering a written appearance personally or by attorney and filing in writing with the court your defenses or objections to the claims set forth against you. You are warned that if you fail to do so the case may proceed without you and a judgment may be entered against you by the court without further notice for any money claimed in the complaint or for any other claim or relief requested by the plaintiff. You may lose money or property or other rights important to you. YOU SHOULD TAKE THIS PAPER TO YOUR LAWYER AT ONCE. IF YOU DONOT HAVE A LAWYER, GO TO OR TELEPHONE THE OFFICE SET FORTH BELOW. THIS OFFICE CAN PROVIDE YOU WITH INFORMATION ABOUT HIRING A LAWYER. IF YOU CANNOT AFFORD TO HIRE A LAWYER, THIS OFFICE MAY BE ABLE TO PROVIDE YOU WITH

INFORMATION ABOUT AGENCIES THAT MAY OFFERLEGAL SERVICES TO ELIGIBLE PERSONS AT A REDUCED FEE OR NO FEE.

AVISO

A USTED SE LE HA DEMANDADO EN LA CORTE. Si usted quiere defenderse contra la demanda expuesta en las siguientes paginas, tiene que tomar accion en un plazo de veinte (20) dlas despues que reciba esta demanda y aviso, por presentar una notificacion de comparecencia escrita personalmente o por un abogado y radicar por eserito en la Corte sus defensas u objeciones a las demandas presentadas en su contra. Se le advierte que si falla en hacerlo, el caso podrla seguir adelante sin usted y un fallo podria ser dictado en su contra por la Corte sin previo aviso por cualquier dinero reclamado en la demanda o por cualquier otro reclamo o desagravio pedido por el/la demandante. Puede que usted pierda dinero o propiedad u. otros derechos importantes para usted. **USTED DEDE LLEVAR ESTE DOCUMENTO A SU ABOGADO INMEDIATAMENTE. SI NO TIBNE ABOGADO, DIRIJASE O LLAME POR TELEFONO A LA OFICINA CUYA DIRECCION SE ENCUENTRA ABAJO. ESTA OFICINA PUEDE PROVEERLE CON INFORMAC16N SOBRE COMO CONTRATAR UN ABOGADO; SI NO TIBNE LOS FONDOS SUFICIBNTES PARA CONTRATAR UN ABOGADO, ESTA OFICINA PODIUA PROPORCIONARLE INFORMACI6N ACERCA DE AGENCIAS QUE PUEDAN OFRECERLES SERVICIOS LEGALES A PERSONAS QUE REUNAN LOS R.EQEQUISITOS A UN HONORARIO REDUCIDO O GRATIS.**

North Penn Legal Services, Inc.

33 N. Main Street, Suite 200 Pittston, PA I8640
(570) 299-4100

(877) 953-4250 Toll free

(570) 824-0001 Fax

101 West Broad Street Suite 513

Hazleton, PA 18201

(570) 455-9512

(877) 953-4250 Toll free

(570)455-3625 Fax

Servicios Legales de North Penn, Inc.
33 la Calle Main de! Norte, Oficina 200
Pittston, PA 18640
(510) 299-4100

(877) 953-4250 Llamada gratuita

(570) 824-0001 Fax

101 la Calle Broad de! Oeste
Oficina513

Hazleton, PA 18201

(570)455-9512

(877) 953-4250 Llamada gratuita

(570) 455-3625 Fax

Kenneth J. Grunfeld
65 Overhill Road
Bala Cynwyd PA 19004
954-525-4100

CLASS ACTION COMPLAINT

Plaintiffs Dean Ambosie, Jenna Balsamello, Nichole Duden, Mackenzie Pawelzik, and Vincent Abbott ("Plaintiffs") bring this Class Action Complaint ("Complaint") against Defendant Wilkes University ("Defendant") as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard Plaintiffs' and Class Members' sensitive personally identifiable information ("PII").[1]

2. Defendant is a private university in Wilkes-Barre, Pennsylvania. It has over 2,300 undergraduate students and over 3,000 graduate students.[2]

3. Defendant detected potentially suspicious activity on a portion of its network environment and through an investigation, on September 22, 2025, Defendant determined that certain networks may have been accessed without authorization between January 25, 2025, and January 26, 2025 (the "Data Breach"). The types of PII accessed during the Data Breach included, but were not limited to, names, addresses, dates of birth, student ID numbers, Social Security numbers, driver's license numbers, state identification numbers, financial account numbers,

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

[2] *Wilkes at a Glance*, WILKES UNIVERSITY, https://www.wilkes.edu/about-wilkes/wilkes-at-a-glance.aspx (last visited Nov. 20, 2025).

financial aid information, health insurance policy numbers, and medical alert information (the "Private Information").[3]

4. On or around October 8, 2025, Defendant began notifying impacted individuals, including Plaintiffs, about the Data Breach ("Notice Letter(s)").

5. Defendant's failure to timely identify and then report the Data Breach made the impacted individuals vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their Private Information.

6. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of the Data Breach.

7. Upon information and belief, Plaintiffs' Private Information is available on the Dark Web as a result of the Data Breach.

8. In failing to adequately protect Plaintiffs' and the Class's Private Information, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state law, federal law, and its own internal privacy policies ("Privacy Policy")[4] and harmed Plaintiffs and Class Members.

9. Plaintiffs and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures.

---

[3] *Data Security Incident Notice*, WILKES UNIVERSITY (Oct. 1, 2025) https://www.wilkes.edu/about-wilkes/policies-and-procedures/data-incident-notice.aspx.

[4] *Privacy Policy*, WILKES UNIVERSITY (revised May 27, 2016), https://www.wilkes.edu/about-wilkes/policies-and-procedures/privacy.aspx (last visited Nov. 20, 2025) ("Wilkes University uses best efforts to secure your personal information from unauthorized access, use or disclosure. The University secures the personally identifiable information you provide on computer servers in a controlled, secure environment, protected from unauthorized access, use or disclosure. When personal information is transmitted to other Web sites, it is protected through the use of encryption, such as the Secure Socket Layer (SSL) protocol.")

10. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have suffered actual and present injuries, including but not limited to: (a) present, certainly impending, and continuing threats of identity theft crimes, fraud, scams, and other misuses of their Private Information; (b) diminution of value of their Private Information; (c) loss of benefit of the bargain (price premium damages); (d) loss of value of privacy and confidentiality of the stolen Private Information; (e) illegal sales of the compromised Private Information; (f) mitigation expenses and time spent responding to and remedying the effects of the Data Breach; (g) identity theft insurance costs; (h) "out of pocket" costs incurred due to actual identity theft; (i) credit freezes/unfreezes; (j) expense and time spent on initiating fraud alerts and contacting third parties; (k) decreased credit scores; (l) lost work time; and (m) anxiety, annoyance, and nuisance; (n) continued risk to their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

11. Accordingly, Plaintiffs, on behalf of themselves and a Class of similarly situated individuals, bring this lawsuit seeking damages, injunctive relief, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

JURISDICTION AND VENUE

12. The Court has subject matter jurisdiction over this action pursuant to 42 Pa. C.S.A. § 931 and 73 Pa. Stat. Ann. § 201-9.2.

13. This Court has personal jurisdiction over Defendant pursuant to 42 Pa. C.S.A. §5301.

14. Venue is proper in this Court is proper pursuant to Pa. R.C.P. No. 2179(a) because

it is where Defendant regularly conducts business and where Defendant's facilities are located.

PARTIES

15. Plaintiff Dean Ambosie is a resident and citizen of Mountain Top, Pennsylvania, where he intends to remain.

16. Plaintiff Jenna Balsamello is a resident and citizen of Pennsylvania, where she intends to remain.

17. Plaintiff Nichole Duden is a resident and citizen of Pennsylvania, where she intends to remain.

18. Plaintiff MacKenzie Pawelzik is a resident and citizen of Pennsylvania, where she intends to remain.

19. Plaintiff Vincent Abbott is a resident and citizen of Virginia, where he intends to remain.

20. Defendant Wilkes University is a private, non-profit institution in Pennsylvania with its principal place of business located in Wilkes-Barre, Pennsylvania.

FACTUAL ALLEGATIONS

A. Defendant's Business

21. Defendant is a private university with over 2,300 undergraduate and over 3,000 graduate students.[5]

22. In the course of their relationship, Plaintiffs and Class Members provided Defendant with their sensitive Private Information.

23. In the course of collecting that Private Information, Defendant promised to provide

[5] *Wilkes at a Glance*, WILKES UNIVERSITY, https://www.wilkes.edu/about-wilkes/wilkes-at-a-glance.aspx (last visited Nov. 20, 2025).

confidentiality and adequate security for the data it collects in accordance with its Privacy Policy.

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 adequate security sufficient 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 the Private Information entrusted to it safe and confidential.

26. Defendant had obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), contract, and industry standards to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

27. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. In fact, in Defendant's Privacy Policy, it states that the Private Information Defendant collects is used for the operation of its services, to maintain the quality of its services, to provide information, for the application process, and to inform of the products, services, or events available from Defendant.[6] Without the required submission of Private Information, Defendant could not have conducted its business.

---

[6] See *Privacy Policy*, WILKES UNIVERSITY (revised May 27, 2016), https://www.wilkes.edu/about-wilkes/policies-and-procedures/privacy.aspx (last visited Nov. 20, 2025) ("Wilkes University takes privacy issues seriously, and will never knowingly share, sell, or rent your personal information with any individual, company, or organization without your advance permission, or unless ordered by a court of law… This information is used by Wilkes University for the operation of the service, to maintain quality of the service, and to provide general statistics regarding use of the Wilkes.edu Web site. Information collected by Wilkes University is used to provide information regarding the university that you request, for the application process and to inform

28. 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.

B. The Data Breach

29. On or about October 8, 2025, Defendant began sending Plaintiffs and other Data Breach victims individualized Notice of Security Incident letters ("Notice Letter(s))."[7]

30. Omitted from the Notice Letters were essential information regarding the Breach, including when Defendant discovered the Data Breach, 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 date, these omitted details have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

31. Defendant also issued a notice of public disclosure about the Data Breach on its website on October 8, 2025, stating:

> Wilkes recently discovered that an unauthorized actor may have gained access to our network environment. Upon learning of this issue, we immediately worked to contain the threat and secure our internal environment. We commenced a prompt and thorough investigation into the incident and worked very closely with external cybersecurity professionals experienced in handling these types of situations to help determine whether any personal or sensitive data, if any, was involved.
>
> After an extensive forensic investigation and manual document review, we discovered on September 22, 2025 that the impacted systems, which were accessed between on or about January 25, 2025

---

you of other products, services or events available from Wilkes University and its official affiliates.") (last accessed Nov. 20, 2025)

[7] *See* Notice of Security Incident letters sent to Plaintiffs by Defendant, attached hereto as **Exhibit A**.

> and on or about January 26, 2025, contained some individuals' personal information. The personal information varies by individual and may include individuals' full name, address, date of birth, student ID number, Social Security number, driver's license number or state identification number, financial account number, financial aid information, health insurance policy number, and/or medical alert information.[8]

32. However, these "disclosures" amount to no real disclosure at all, as they fail 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.

33. Defendant had obligations created by the FTCA, contract, common law, and industry standards to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

34. 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.

35. The attacker accessed and acquired files containing unencrypted Private Information of Plaintiffs and Class Members. Plaintiffs' and Class Members' Private Information was accessed and stolen in the Data Breach.

36. Plaintiffs further believe that their 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.

C. Defendant Acquires, Collects, and Stores Plaintiffs' and the Class's Private Information

[8] *Data Security Incident Notice*, WILKES UNIVERSITY (Oct. 8, 2025), https://www.wilkes.edu/about-wilkes/policies-and-procedures/data-incident-notice.aspx (last visited Nov. 20, 2025).

37. As part of its business, Defendant acquires sensitive Private Information.

38. Defendant retains and stores this information and derives a substantial economic benefit from the Private Information that they collect. But for the collection of Plaintiffs' and Class Members' Private Information, Defendant would be unable to operate its business.

39. 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 it was responsible for protecting the Private Information from disclosure.

40. 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.

41. 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.

42. Defendant's negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

D. Defendant Failed to Comply with Regulatory Requirements and Standards

43. Federal and state regulators have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and employees. There are a number of state and federal laws, requirements, and industry standards governing the protection of Private Information.

44. For example, at least 24 states have enacted laws addressing data security practices that require businesses that own, license, or maintain Private Information about a resident of that state to implement and maintain "reasonable security procedures and practices" and to protect Private Information from unauthorized access.

45. Additionally, cybersecurity firms have promulgated a series of best practices that at a minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting of physical security systems; protecting against any possible communication system; and training staff regarding critical points.[9]

46. The FTC has issued several guides for businesses, highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be considered for all business decision-making.[10]

47. Under the FTC's 2016 *Protecting Personal Information: Guide for Business* publication, the FTC notes that businesses should safeguard the personal customer information they retain; properly dispose of unnecessary personal information; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to rectify security issues.[11]

48. The guidelines also suggest that businesses use an intrusion detection system to expose a breach as soon as it happens, monitor all incoming traffic for activity indicating someone

---

[9] *See Addressing BPO Information Security: A Three-Front Approach*, DATAMARK, INC. (Nov. 2016), https://insights.datamark.net/addressing-bpo-information-security.
[10] *Start With Security*, FED. TRADE COMM'N ("FTC"), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[11] *Protecting Personal Information: A Guide for Business*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

is trying to hack the system, watch for large amounts of data being siphoned from the system, and have a response plan in the event of a breach.

49. The FTC advises companies to not keep information for periods of time longer than needed to authorize a transaction, restrict access to private information, mandate complex passwords to be used on networks, utilize industry-standard methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[12]

50. The FTC has brought enforcement actions against companies for failing to adequately and reasonably protect consumer data, treating the failure to do so as an unfair act or practice barred by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders originating from these actions further elucidate the measures businesses must take to satisfy their data security obligations.

51. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

52. Defendant's failure to verify that it had implemented reasonable security measures constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

E. Defendant Failed to Comply with Industry Practices

53. Various cybersecurity industry best practices have been published and should be consulted as a go-to resource when developing an organization's cybersecurity standards. The Center for Internet Security ("CIS") promulgated its Critical Security Controls, which identify the most commonplace and essential cyber-attacks that affect businesses every day and proposes

[12] *Id.*

solutions to defend against those cyber-attacks.[13] All organizations collecting and handling Private Information, such as Defendant, are strongly encouraged to follow these controls.

54. Further, the CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.[14]

55. Several best practices have been identified that a minimum should be implemented by companies like Defendant, including but not limited to securely configuring business software, managing access controls and vulnerabilities to networks, systems, and software, maintaining network infrastructure, defending networks, adopting data encryption while data is both in transit and at rest, and securing application software.[15]

56. Defendant failed to follow these and other industry standards to adequately protect the Private Information of Plaintiffs and Class Members.

F. Defendant Owed Plaintiffs and Class Members a Common Law Duty to Safeguard their Private Information

57. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant's duty owed to Plaintiffs and Class Members obligated it to provide reasonable data security, including consistency with industry standards and requirements, and to ensure its computer systems,

---

[13] CENTER FOR INTERNET SECURITY, *Critical Security Controls*, at 1 (May 2021), https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf.
[14] *See CIS Benchmarks FAQ*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/.
[15] *See* CENTER FOR INTERNET SECURITY, *Critical Security Controls* (May 2021), https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf.

networks, and protocols adequately protected Plaintiffs' and Class Members' Private Information.

58. Defendant owed a duty to Plaintiffs and Class Members to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees and others who accessed Private Information within its computer systems on how to adequately protect Private Information.

59. Defendant owed a duty to Plaintiffs and Class Members to implement processes that would detect a compromise of Private Information in a timely manner and act upon data security warnings and alerts in a timely fashion.

60. Defendant owed a duty to Plaintiffs and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

61. Defendant owed a duty of care to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

62. Defendant failed to take the necessary precautions required to safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure. Defendant's actions and omissions represent a flagrant disregard of Plaintiffs' and Class Members' rights.

G. Defendant Could Have Prevented the Data Breach

63. Data breaches are preventable.[16] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[17] he added that "[o]rganizations that collect, use, store, and share sensitive

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

personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[18]

64. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[19]

65. In a data breach like this, many failures laid the groundwork for the Data Breach.

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

67. 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.20

68. 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.

69. 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.

---

[18] *Id.* at 28.

[19] *Id.*

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

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

71. 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 reasonable cybersecurity readiness.

72. 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."21

73. To prevent the Data Breach, Defendant could and should have implemented, as recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.

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

- 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.
- 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.[22]

74. Further, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

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

[22] *Id.* at 3–4.

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

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

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

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

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic....[23]

75. In addition, 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;

- **Build credential hygiene**

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

- 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].[24]

76. Given that Defendant was storing the Private Information of thousands of individuals, Defendant could have and should have implemented all of the above measures to prevent and detect cyberattacks.

77. 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.[25]

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

79. The FTC, among others, has repeatedly emphasized the importance of disposing of unnecessary Private Information, saying simply: "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.

---

[24] *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/.

[25] *See, e.g.,* Adnan Raja, *How to Safeguard Your Business Data with Encryption*, FORTRA (Aug. 14, 2018), https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption.

If it's not on your system, it can't be stolen by hackers."[26] Defendant, rather than following this basic standard of care, kept thousands of individuals' unencrypted Private Information indefinitely.

80. In sum, the Data Breach could have readily been prevented through the use of industry standard network segmentation and encryption of all Private Information.

81. Further, the scope of the Data Breach could have been dramatically reduced had Defendant utilized proper record retention and destruction practices.

H. Plaintiffs and Class Members Suffered Common Injuries and Damages due to Defendant's Conduct

82. Defendant's failure to implement or maintain adequate data security measures for Plaintiffs' and Class Members' Private Information directly and proximately injured Plaintiffs and Class Members by the resulting disclosure of their Private Information in the Data Breach.

83. 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.

84. Plaintiffs and Class Members are also at a continued risk because their Private Information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect the Private Information in its systems.

85. As a result of Defendant's delay between the identification of the Data Breach, which occurred as early as January 25, 2025, and the notice of the Data Breach sent to affected

[26] *Protecting Personal Information: A Guide for Business*, FTC, *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf, at p. 6.

persons in October 2025, the risk of fraud for Plaintiffs and Class Members increased exponentially.

86. As a result of Defendant's ineffective and inadequate data security practices, the resulting Data Breach, and the foreseeable consequences of their Private Information ending up in criminals' possession, the risk of identity theft to Plaintiffs and Class Members has materialized and is imminent, and they have all sustained actual injuries and damages, including, without limitation, (a) invasion of privacy; (b) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) deprivation of value of their Private Information; (g) loss of the benefit of their bargain with Defendant; (h) emotional distress including anxiety and stress in dealing with the Data Breach's aftermath; and (i) the continued risk to their sensitive 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 it collects and maintains.

The Risk of Identity Theft to Plaintiffs and Class Members is Present and Ongoing

87. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach.

88. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[27] 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 "[n]ame, Social Security number, date of

[27] 17 C.F.R. § 248.201 (2013).

birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[28]

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

90. The dark web is an unindexed layer of the internet that requires special software or authentication to access. 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. This prevents dark web marketplaces from being easily monitored by authorities or accessed by those not in the know.

91. A sophisticated black market exists on the dark web where criminals can buy or sell malware, firearms, drugs, and frequently, personal and medical information like the Private Information at issue here. 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 medical information. As Microsoft

[28] *Id.*

warns "[t]he anonymity of the dark web lends itself well to those who would seek to do financial harm to others."[29]

92. The unencrypted Private Information of Plaintiffs and Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted and detailed Private Information may fall into the hands of companies that will use it for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the Plaintiffs' and Class Members' Private Information.

93. 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 to track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

94. 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 are often the starting point for these additional targeted attacks on the victims.

95. Identity thieves can also use an individual's personal data and Private Information to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a

[29] *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 Nov. 20, 2025).

fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's information, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant issued in the victim's name.[30]

96. One such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[31]

97. 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 to assemble complete dossiers on individuals.

98. 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

---

[30] *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMINISTRATION, 1 (2018), https://www.ssa.gov/pubs/EN-05-10064.pdf.

[31] "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 Nov. 20, 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.

99. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

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

101. The development of "Fullz" packages means that 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. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that their stolen Private Information is being misused, and that such misuse is traceable to the Data Breach.

102. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice:

> A direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss.[32]

103. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

---

[32] Erika Harrell, *Bureau of Just. Stat.*, U.S. DEP'T OF JUST., NCJ 256085, *Victims of Identity Theft*, 2018 I (2020) https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last visited Nov. 20, 2025).

104. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims must spend a considerable time repairing the damage caused by the theft of their Private Information. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

105. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Private Information. To protect themselves, Plaintiffs and Class Members will need to remain vigilant for years or even decades to come.

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

106. 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 of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the asset of time has been lost.

107. In the event that Plaintiffs and Class Members 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."

108. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must monitor their financial accounts for many years to mitigate that harm.

109. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover.

110. These efforts are 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), 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.[33]

111. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct that caused the Data Breach.

Diminished Value of Private Information

112. Personal data like Private Information is a valuable property right.[34] 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.

---

[33] *See* FEDERAL TRADE COMMISSION, *Identity Theft.gov*, https://www.identitytheft.gov/Steps

[34] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PRIVATE INFORMATION") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PRIVATE INFORMATION, 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).

113. 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.

114. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and black markets, has been damaged and diminished in its value by its unauthorized and likely release onto the dark web, where it holds significant value for the threat actors.

115. 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.

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

116. To date, Defendant has done little to provide Plaintiffs and Class Members with relief for the damages they have suffered due to the Data Breach.

117. Given the breach, the type of information involved, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the 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; filing false tax returns; taking out loans or insurance; or filing false unemployment claims.

118. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected

fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

119. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer's data breach, where victims can easily cancel their cards and request a replacement. The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as Social Security numbers).

120. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future.

121. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

Loss of Benefit of the Bargain

122. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain.

123. Plaintiffs and Class Members understood and expected that Defendant maintained adequate data security to protect the Private Information they were required to provide.

124. 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 struck with Defendant.

Plaintiff Dean Ambosie's Experience

125. Plaintiff Ambosie is a former student of Defendant.

126. In the course of Defendant's regular business operation, Plaintiff Ambosie was required to provide his Private Information to Defendant.

127. At the time of the Data Breach, Defendant maintained Plaintiff Ambosie's Private Information in its system.

128. Through its inadequate security practices, Defendant exposed Plaintiff Ambosie's Private Information for theft and sale on the dark web.

129. Plaintiff Ambosie reasonably understood that a portion of the tuition paid to Defendant would be used to pay for adequate cybersecurity and protection of Private Information.

130. Plaintiff Ambosie is very careful about sharing his sensitive Private Information. Plaintiff Ambosie 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. Plaintiff Ambosie would not have entrusted his Private Information to Defendant had he known of Defendant's lax data security policies.

131. Plaintiff Ambosie received the Notice Letter, dated October 8, 2025, by U.S. mail. According to the Notice Letter, Plaintiff Ambosie's Private Information was improperly accessed and obtained by unauthorized third parties, including his date of birth, taxpayer ID number, student ID number, home address, financial information, home phone number, class list, and Social Security number.[35]

132. As a result of the Data Breach, Plaintiff Ambosie made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach. Plaintiff Ambosie has spent significant time dealing with the Data Breach—valuable

[35] *See* Ex. A.

time Plaintiff Ambosie 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.

133. Plaintiff Ambosie suffered actual injury from having his Private Information compromised as a result of the Data Breach 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) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) 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.

134. The Data Breach has caused Plaintiff Ambosie 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.

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

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

137. Plaintiff Ambosie 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 Jenna Balsamello's Experience

138. Plaintiff Balsamello is a former student of Defendant.

139. Thus, Defendant obtained and maintained Plaintiff Balsamello's Private Information.

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

141. Plaintiff Balsamello is very careful about the privacy and security of her Private Information. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

142. Plaintiff Balsamello provided her 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. Defendant obtained and continues to maintain Plaintiff Balsamello's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

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

144. Plaintiff Balsamello received a Notice of Data Breach on or around October 17, 2025.

145. Thus, on information and belief, Plaintiff Balsamello's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

146. Through its Data Breach, Defendant compromised Plaintiff Balsamello's Private Information.

147. Plaintiff Balsamello ***already suffered*** from identity theft and fraud—whereby cybercriminals placed fraudulent charges of approximately $300 on her debit card in or around January 2025. Thereafter, Plaintiff Balsamello spent time disputing the fraud with her bank and filing a police report.

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

149. And in the aftermath of the Data Breach, Plaintiff Balsamello suffered from a spike in spam and scam phone calls (approximately 10–12 per day).

150. Plaintiff Balsamello fears for her personal financial security and worries about what information was exposed in the Data Breach.

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

152. Plaintiff Balsamello suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy.

153. Plaintiff Balsamello suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

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

155. Because of the Data Breach, Plaintiff Balsamello anticipates spending considerable amounts of time and money to try and mitigate her injuries.

156. Today, Plaintiff Balsamello has a continuing interest in ensuring that her Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Nichole Duden's Experiences

157. Plaintiff Duden provided Defendant with her sensitive Private Information as a condition of her enrollment at Defendant's university.

158. After Plaintiff Duden left Defendant's university, Defendant suffered a Data Breach.

159. Plaintiff Duden received notice of the Data Breach around October 8, 2025, informing her that her Private Information may have been either accessed and/or acquired by an unauthorized individual including Plaintiff Duden's "date of birth, social security number, student ID number, home address, home phone number, email address, and financial aid information."[36]

160. Plaintiff Duden is especially alarmed by the amount of stolen or accessed Private Information listed on Defendant's letter. Despite Defendant providing that list, she cannot be sure more of her Private Information was exfiltrated. Now she checks her bank accounts and credit cards throughout the day each day, spending approximately an hour per week just monitoring accounts because of Defendant's Data Breach.

161. Plaintiff Duden provided her Private Information to Defendant and trusted it would use reasonable measures to protect it according to Defendant's Privacy Policy, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Duden's Private Information

[36] *Id.*

and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

162. Plaintiff Duden reasonably understood that a portion of the tuition paid to Defendant would be used to pay for adequate cybersecurity and protection of Private Information.

163. Through its inadequate security practices, Defendant exposed Plaintiff Duden's Private Information for theft and sale on the dark web. On or about February 11, 2025, an unauthorized third party accessed Plaintiff Duden's savings account, resulting in an approximately $50 in-store purchase at Walmart that mimicked a legitimate transaction she made the same day. Her financial institution traced the fraudulent activity to Bentonville, Arizona. Plaintiff Duden incurred a $5 fee as a result of the unauthorized transaction before her bank refunded the full $55 following its investigation. Plaintiff Duden was advised to cancel her debit card, obtain a replacement card, and she spent approximately one hour working with bank representatives to mitigate this issue and secure her account.

164. Plaintiff Duden is very careful about sharing her sensitive Private Information. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Duden also stores any documents containing her sensitive information in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for his various online accounts. In or around June 2025, Plaintiff Duden received a credit-monitoring alert advising her that her PII had been used in connection with an individual using an unfamiliar first and last name. After enrolling in the complimentary credit-monitoring services offered following the breach, Plaintiff Duden discovered a hard credit inquiry from an unfamiliar entity, COAF, which she is disputing because she has never applied for any personal loan.

165. Plaintiff Duden has already spent much time monitoring her accounts to protect herself and will continue to spend significant time and effort monitoring her accounts to protect herself from identity theft. In October 2025, Plaintiff Duden received a notification from Facebook regarding an unusual login attempt on her account, prompting her to change all usernames and passwords and implement additional security measures.

166. Plaintiff Duden knows that cybercriminals often sell Private Information, and that her Private Information could be abused months or even years after a data breach.

167. Had Plaintiff Duden been aware that Defendant's computer systems were not secure, she would not have entrusted Defendant with her personal data.

168. Plaintiff Duden suffered actual injury from the exposure and theft of her Private Information—which violates her rights to privacy.

169. Plaintiff Duden suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

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

171. Today, Plaintiff Duden has a continuing interest in ensuring that her Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff MacKenzie Pawelzik's Experiences

172. Defendant obtained Plaintiff Pawelzik's Private Information with the reasonable expectation and mutual understanding that Defendant would keep her Private Information secure

from unauthorized access.

173. Defendant was in possession of Plaintiff Pawelzik's Private Information before, during, and after the Data Breach.

174. Following the Data Breach, Plaintiff Pawelzik made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching the Data Breach, reviewing and monitoring her accounts for fraudulent activity, and reviewing her credit reports. In total, Plaintiff Pawelzik estimates she has already spent several hours a week responding to the Data Breach.

175. Plaintiff Pawelzik will be forced to spend additional time reviewing her credit reports and monitoring her accounts for the rest of her life. This is time spent, which has been lost forever and cannot be recaptured.

176. Plaintiff Pawelzik places significant value in the security of her Private Information and does not readily disclose it. Plaintiff Pawelzik entrusted Defendant with her Private Information with the understanding that Defendant would keep her information secure and would employ reasonable and adequate data security measures to ensure that her Private Information would not be compromised.

177. Plaintiff Pawelzik has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

178. As a direct and traceable result of the Data Breach, Plaintiff Pawelzik suffered actual injury and damages after her Private Information was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring her accounts and credit reports for fraudulent activity; (b) loss of privacy due to her Private Information being accessed and stolen by cybercriminals; (c) loss of the benefit of her bargain because Defendant did

not adequately protect her Private Information; (d) emotional distress because identity thieves now possess her sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that her Private Information has been stolen and published on the dark web; (f) diminution in the value of her Private Information, a form of intangible property that Defendant obtained from Plaintiff Pawelzik; and (g) other economic and non-economic harm.

179. Plaintiff Pawelzik has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. This risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the Private Information stolen in the Data Breach.

180. Plaintiff Pawelzik has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiff Pawelzik's Private Information will be wholly unprotected and at-risk of future data breaches.

Plaintiff Vincent Abbott's Experiences

181. Plaintiff Abbott provided his Private Information indirectly and/or directly to Defendant, and that Private Information was compromised during the Data Breach.

182. Defendant obtained Plaintiff Abbott's Private Information with the reasonable expectation and mutual understanding that Defendant would keep his Private Information secure from unauthorized access.

183. Defendant was in possession of Plaintiff Abbott's Private Information before, during, and after the Data Breach.

184. Through its inadequate security practices, Defendant exposed Plaintiff Abbott's Private Information for theft and sale on the dark web.

185. Following the Data Breach, Plaintiff Abbott made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching the Data Breach, reviewing and monitoring his accounts for fraudulent activity, and reviewing his credit reports.

186. Plaintiff Abbott will be forced to spend additional time reviewing his credit reports and monitoring his accounts for the rest of his life. This is time spent, which has been lost forever and cannot be recaptured.

187. Plaintiff Abbott places significant value in the security of his Private Information and does not readily disclose it. Plaintiff Abbott entrusted Defendant with his Private Information with the understanding that Defendant would keep his information secure and would employ reasonable and adequate data security measures to ensure that his Private Information would not be compromised.

188. Plaintiff Abbott has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

189. As a direct and traceable result of the Data Breach, Plaintiff Abbott suffered actual injury and damages after his Private Information was compromised and stolen in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts and credit reports for fraudulent activity; (b) loss of privacy due to his Private Information being accessed and stolen by cybercriminals; (c) loss of the benefit of her bargain because Defendant did not adequately protect his Private Information; (d) emotional distress because identity thieves now possess his sensitive information; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his Private Information has been stolen and published on the dark web; (f) diminution in the value of his Private Information, a form of intangible property that Defendant obtained from Plaintiff Abbott; and (g) other economic and non-economic harm.

190. Plaintiff Abbott has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. This risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the Private Information stolen in the Data Breach.

191. Plaintiff Abbott has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiff Abbott's Private Information will be wholly unprotected and at-risk of future data breaches.

CLASS ALLEGATIONS

192. Pursuant to Rules 1702, 1708, and 1709 of the Pennsylvania Rules of Civil Procedure, Plaintiffs bring this action on behalf of themselves and on behalf of all members of the proposed class defined as:

> All individuals residing in the United States whose Private Information was compromised in the Data Breach ("Class").

193. 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.

194. Plaintiffs reserve the right to amend the definition of the proposed Class or to add a subclass before the Court determines whether certification is appropriate.

195. **Numerosity – Pennsylvania Rule of Civil Procedure 1702(1).** The Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, Plaintiffs believe the proposed Class includes thousands of individuals who have been

damaged by Defendant's conduct as alleged herein. The precise number of Class Members is unknown to Plaintiffs but may be ascertained from Defendant's records.

196. **Commonality – Pennsylvania Rule of Civil Procedure 1702(2).** 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:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant's conduct violated the FTCA;

c. When Defendant learned of the Data Breach;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

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

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

g. Whether Defendant owed duties to Class Members to safeguard their Private Information;

h. Whether Defendant breached their duties to Class Members to safeguard their Private Information;

i. Whether hackers obtained Class Members' Private Information via the Data Breach;

j. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

k. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

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

m. What damages Plaintiffs and Class Members suffered as a result of Defendant's misconduct;

n. Whether Defendant's conduct was negligent;

o. Whether Defendant breached contracts it had with Plaintiffs and Class Members;

p. Whether Defendant was unjustly enriched;

q. Whether Plaintiffs and Class Members are entitled to damages;

r. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

s. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

197. **Typicality – Pennsylvania Rule of Civil Procedure 1702(3).** Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, inter alia, all Class Members were injured through the common misconduct of Defendant. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to

Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

198. **Adequacy of Representation – Pennsylvania Rule of Civil Procedure 1702(4) and 1709.** Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel are competent and experienced in litigating class actions, including data privacy litigation of this kind.

199. **Predominance – Pennsylvania Rule of Civil Procedure 1708(a)(1).** Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members. For example, all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated 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.

200. **Manageability – Pennsylvania Rule of Civil Procedure 1708(a)(2).** While the precise size of the Class is unknown without the disclosure of Defendant's records, public records indicate that thousands of individuals' Private Information was compromised in the Data Breach. The claims of Plaintiffs and Class Members are substantially identical as explained above. Certifying the case as a class action will centralize these substantially identical claims in a single proceeding and adjudicating these substantially identical claims at one time is the most manageable litigation method available to Plaintiffs and Class Members.

201. **Risk of Inconsistent, Varying or Prejudicial Adjudications – Pennsylvania Rule of Civil Procedure 1708(a)(3).** If the claims of Plaintiffs and Class Members were tried separately, Defendant may be confronted with incompatible standards of conduct and divergent

court decisions. Furthermore, if the claims of Plaintiffs and Class Members were tried individually, adjudications with respect to individual Class Members and the propriety of their claims could be dispositive on the interests of Class Members not party to those individual adjudications and substantially, if not fully, impair or impede their ability to protect their interests.

202. **Litigation Already Commenced – Pennsylvania Rule of Civil Procedure 1708 (a)(4).** To Plaintiffs' knowledge, there are no other cases that have been brought against Defendant, or that are currently pending against Defendant, where a Pennsylvania consumer seeks to represent a class of Pennsylvania residents based on the Data Breach or the conduct alleged in this Class Action Complaint.

203. **The Appropriateness of the Forum – Pennsylvania Rule of Civil Procedure 1708 (a)(5).** This is the most appropriate forum to concentrate the litigation because Defendant is headquartered in this county and does business in the county, and a substantial amount of injury-causing conduct occurred in this county.

204. **The Class Members' Claims Support Certification – Pennsylvania Rule of Civil Procedure 1708(a)(6) and (7).** Given the relatively low amount recoverable by each Class Member, the expenses of individual litigation are insufficient to support or justify individual suits. Furthermore, the damages that may be recovered by Class Members will not be so small such that class certification is unjustified.

205. **The General Applicability of Defendant's Conduct – Pennsylvania Rule of Civil Procedure 1708(b)(2).** Defendant's failure to secure Private Information is generally applicable to the Class as a whole, making equitable and declaratory relief appropriate with respect to each Class Member.

206. Finally, all members of the proposed Class are readily ascertainable. Defendant has

access to the names and addresses and/or email addresses of Class Members affected by the Data Breach.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

207. Plaintiffs restate and reallege paragraphs 1 through 206 set forth above as if fully alleged herein.

208. Defendant requires individuals, including Plaintiffs and Class Members, to submit non-public Private Information in the ordinary course of operating its business.

209. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of its business.

210. Plaintiffs and Class Members entrusted Defendant with their Private Information, directly or indirectly, with the understanding that Defendant would safeguard their information.

211. 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.

212. 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.

213. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 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.

214. Defendant's duty to use reasonable security measures also arose under the GLBA, under which they were required to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards

215. 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.

216. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant, Plaintiffs and Class Members. That special relationship arose because Plaintiffs and Class Members entrusted Defendant with their confidential Private Information, a necessary part of doing business with Defendant, either as a student or otherwise.

217. 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.

218. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or Class Members.

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

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

221. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and Class Members 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 Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

222. 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 remove Private Information it was no longer required to retain pursuant to regulations; and

e. 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.

223. 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 Class Members.

224. 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 these statutes were intended to guard against.

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

226. 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 Class Members.

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

228. 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 in the Defendant's industry.

229. Defendant has 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.

230. Plaintiffs and Class Members 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 Class Members,

the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

231. 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.

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

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

234. Defendant's duty extended to protecting Plaintiffs and Class Members 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* Rest. (2d) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

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

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

237. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and Class Members and the harm, or risk of imminent harm, suffered by Plaintiffs and Class Members. The Private Information of

Plaintiffs and Class Members 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.

238. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) 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.

239. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members 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.

240. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members 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.

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

242. 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.

243. 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
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

244. Plaintiffs restate and reallege paragraphs 1 through 206 set forth above as if fully alleged herein.

245. Plaintiffs and Class Members entrusted their Private Information to Defendant as a condition of receiving employment or enrollment with Defendant. In so doing, Plaintiffs and Class Members 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 Plaintiffs and Class Members if their data had been breached and compromised or stolen.

246. At the time Defendant acquired the Private Information of Plaintiffs and Class Members, 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.

247. Implicit in the agreements between Plaintiffs 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 Plaintiffs 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 Plaintiffs and Class Members from unauthorized disclosure or uses, and (f) retain the Private Information only under conditions that kept such information secure and confidential.

248. Plaintiffs and Class Members 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, not delete the Private Information that Defendant no longer had a reasonable need to maintain.

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

250. Defendant breached the implied contracts they made with Plaintiffs and Class Members by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiffs and Class Members once the relationship ended, and by failing to provide timely and accurate notice to them that their personal information was compromised because of the Data Breach.

251. As a direct and proximate result of Defendant's breach of implied contracts, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) 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.

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

COUNT III
Breach Of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

253. Plaintiffs restate and reallege paragraphs 1 through 206 above as if fully set forth herein.

254. In providing their Private Information, directly or indirectly, to Defendant, Plaintiffs and Class Members justifiably placed a special confidence in Defendant to act in good faith and with due regard to the interests of Plaintiffs and Class Members to safeguard and keep confidential that Private Information.

255. Defendant accepted the special confidence Plaintiffs and Class Members placed in it, as evidenced by its assertion that it is committed to protecting the privacy of Plaintiffs' and Class Members' personal information.

256. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became a 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 the benefit of Plaintiffs and Class Members, for the safeguarding of Plaintiffs and Class Member's Private Information.

257. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of their relationship with Defendant, in particular, to keep secure the Private Information of Plaintiffs and Class Members.

258. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

259. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

260. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of Private Information; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) 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.

261. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT IV
Unjust Enrichment / Quasi Contract
(On Behalf of Plaintiffs and the Class)

262. Plaintiffs restate and reallege paragraphs 1 through 206 above as if fully set forth herein.

263. This count is brought in the alternative to Plaintiffs' breach of implied contract claim.

264. Plaintiffs and Class Members conferred a monetary benefit on Defendant, by providing Defendant with their valuable Private Information. In conferring this benefit, Plaintiffs 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.

265. Defendant appreciated that Plaintiffs and Class Members were conferring a benefit upon it and accepted that monetary benefit.

266. Acceptance of the benefit under the facts and circumstances described herein makes it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

267. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary value of the benefit belonging to Plaintiffs and Class Members,

because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

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

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

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

271. 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) actual identity theft; (ii) the loss of the opportunity 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 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 Private Information in their 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 Plaintiffs and Class Members.

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

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

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Class, 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;

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 provide 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 Plaintiffs' and Class Members' respective lifetimes;

v. 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;

vi. prohibiting Defendant from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;

vii. 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;

viii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

ix. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

x. requiring Defendant to segment data by, among other things, creating firewalls and controls so that if one area of Defendant's network is compromised, hackers cannot gain access to portions of Defendant's systems;

xi. requiring Defendant to conduct regular database scanning and security checks;

xii. 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;

xiii. requiring Defendant to routinely and continually conduct internal training and education, 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;

xiv. requiring Defendant to implement a system of tests to assess its respective 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;

xv. 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;

xvi. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal

identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvii. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xviii. 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, statutory, consequential, and punitive damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses 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.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all claims so triable.

Dated: November 20, 2025

Respectfully submitted,

By: */s/ Kenneth J. Grunfeld*
Kenneth J. Grunfeld (PA Bar # 84121)
Courtney Maccarone*
KOPELOWITZ OSTROW P.A.
65 Overhill Road
Bala Cynwyd, PA 19004
Tel: (954) 332-4200
grunfeld@kolawyers.com
maccarone@kolawyers.com

Leanna A. Loginov*
SHAMIS & GENTILE, P.A.

14 NE 1st Ave, Suite 705
Miami, FL 33132
Tel: (305) 479-2299
lloginov@shamisgentile.com

Samuel J. Strauss*
Raina C. Borrelli*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
Tel: (872) 263-1100
Fax: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com

Leigh Montgomery*
EKSM, LLP
4200 Montrose Blvd., Ste. 200
Houston, Texas 77006
Tel: (888) 350-3931
lmontgomery@eksm.com

Mariya Weekes*
Mark Svensson*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
333 SE 2nd Avenue, Suite 2000
Miami, FL 33131
Tel: (866) 252-0878
mweekes@milberg.com
msvensson@milberg.com

Gerald D. Wells, III (PA Bar # 88277)
Stephen E. Connolly*
LYNCH CARPENTER LLP
1760 Market Street, Suite 600
Philadelphia, PA 19103
Tel: 267-609-6910
Fax: 267-609-6955
jerry@lcllp.com
steve@lcllp.com

Attorneys for Plaintiffs and the Putative Class

** pro hac vice forthcoming*

IN THE COURT OF COMMON PLEAS OF LUZERNE COUNTY, PENNSYLVANIA

DEAN AMBOSIE, MARIA GRANDINETTI, NICHOLE DUDEN, MACKENZIE PAWELSIK, AUTUMN and VINCENT ABBOTT, individually and on behalf of all others similarly situated, Plaintiffs, v. WILKES UNIVERSITY, Defendant.	Case No.: _____ **JURY TRIAL DEMANDED**

VERIFICATION

I, Dean Ambosie, hereby verify that I am a plaintiff in the above-captioned matter and the allegations set forth in the complaint are true and correct, to the best of my knowledge, information and belief, subject to the 18 Pa.CS § 4904.

Dated: 11 / 19 / 2025

_____
Dean Ambosie

IN THE COURT OF COMMON PLEAS OF LUZERNE COUNTY, PENNSYLVANIA

DEAN AMBOSIE, MARIA GRANDINETTI, NICHOLE DUDEN, MACKENZIE PAWELSIK, AUTUMN and VINCENT ABBOTT, individually and on behalf of all others similarly situated, Plaintiffs, v. WILKES UNIVERSITY, Defendant.	Case No.: _____ **JURY TRIAL DEMANDED**

VERIFICATION

I, Nichole Duden, hereby verify that I am a plaintiff in the above-captioned matter and the allegations set forth in the complaint are true and correct, to the best of my knowledge, information and belief, subject to the 18 Pa.CS § 4904.

Dated: Nov 14, 2025

Nichole Lee Duden (Nov 14, 2025 16:40:32 EST)

Nichole Duden

IN THE COURT OF COMMON PLEAS OF LUZERNE COUNTY, PENNSYLVANIA

DEAN AMBOSIE, MARIA GRANDINETTI, NICHOLE DUDEN, MACKENZIE PAWELSIK, AUTUMN and VINCENT ABBOTT, individually and on behalf of all others similarly situated, Plaintiffs, v. WILKES UNIVERSITY, Defendant.	Case No. _____ **JURY TRIAL DEMANDED**

VERIFICATION

I, Jenna Balsamello, hereby verify that I am a plaintiff in the above-captioned matter and the allegations set forth in the complaint are true and correct, to the best of my knowledge, information and belief, subject to the 18 Pa.CS § 4904.

Dated: 11 / 19 / 2025

Jenna Balsamello

IN THE COURT OF COMMON PLEAS OF LUZERNE COUNTY, PENNSYLVANIA

DEAN AMBOSIE, MARIA GRANDINETTI, NICHOLE DUDEN, MACKENZIE PAWELSIK, AUTUMN BULLEK and VINCENT ABBOTT, individually and on behalf of all others similarly situated, Plaintiffs, v. WILKES UNIVERSITY, Defendant.	Case No.:_____ **JURY TRIAL DEMANDED**

VERIFICATION

I, Vincent Abbott, hereby verify that I am a plaintiff in the above-captioned matter and the allegations set forth in the complaint are true and correct, to the best of my knowledge, information and belief, subject to the 18 Pa.CS § 4904.

Dated: 11/20/2025

DocuSigned by:
Vincent Abbott
8C12ADBE650E495...

Vincent Abbott

IN THE COURT OF COMMON PLEAS OF LUZERNE COUNTY, PENNSYLVANIA

DEAN AMBOSIE, MARIA GRANDINETTI, NICHOLE DUDEN, MACKENZIE PAWELZIK, AUTUMN and VINCENT ABBOTT, individually and on behalf of all others similarly situated, Plaintiffs, v. WILKES UNIVERSITY, Defendant.	Case No.: _____ **JURY TRIAL DEMANDED**

VERIFICATION

I, Mackenzie Pawelzik, hereby verify that I am a plaintiff in the above-captioned matter and the allegations set forth in the complaint are true and correct, to the best of my knowledge, information and belief, subject to the 18 Pa.CS § 4904.

Dated: 19/11/2025

Mackenzie Pawelzik (Nov 19, 2025 12:14:09 EST)

Mackenzie Pawelzik