IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

CHRISTOPHER F. KELLY, on behalf of himself and on behalf of all other similarly situated individuals, Plaintiff, v. **UNIVERSITY OF PENNSYLVANIA**, Defendant.	Case No. 2:25-cv-6234 **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Christopher F. Kelly ("Plaintiff"), individually and on behalf of all other similarly situated individuals (the "Class" or "Class Members," as defined below), by and through his undersigned counsel, files this Class Action Complaint against the University of Pennsylvania ("UPenn" or "Defendant") and alleges the following based on personal knowledge of facts, upon information and belief, and based on the investigation of his counsel as to all other matters.

I. NATURE OF THE ACTION

1. Plaintiff brings this class action lawsuit against UPenn for its failure to protect and safeguard Plaintiff's and the Class's highly sensitive personally identifiable information ("PII"). As a result of UPenn's negligence and insufficient data security, cybercriminals easily infiltrated Defendant's inadequately protected email accounts on or around October 31, 2025, and accessed the PII of Plaintiff and the Class (the "Data Breach"

or "Breach"). Now, Plaintiff's and the Class's PII is in the hands of cybercriminals who will undoubtedly use their PII for nefarious purposes for the rest of their lives.

2. UPenn is a private institution of higher learning located within the City and County of Philadelphia, Pennsylvania. UPenn offers academic degrees in a variety of disciplines.

3. As part of its business, and in order to gain profits, UPenn obtained and stored the personal information of its students, applicants, and faculty, including the personal information of Plaintiff and Class members.

4. By taking possession and control of Plaintiff's and Class members' PII, UPenn assumed a duty to securely store and protect it.

5. Upon information and belief, Plaintiff and the Class are current and former students and employees of UPenn.

6. On October 31, 2025, UPenn identified unauthorized remote access to several UPenn owned email accounts.[1] A series of mass emails were sent to students, faculty, alumni, and parents from accounts linked to the Graduate School of Education.[2] In the series of emails, the unknown actors stated "all your data will be leaked."[3] Other Penn affiliates have received the email multiple times from different senders with official "@upenn.edu" email addresses.[4]

---

[1] *See* https://www.thedp.com/article/2025/10/penn-gse-emails-we-got-hacked-subject-security-breach (last visited Oct. 31, 2025).
[2] *Id.*
[3] *See* https://techcrunch.com/2025/10/31/hackers-threaten-to-leak-data-after-breaching-university-of-pennsylvania-to-send-mass-emails/ (last visited Oct. 31, 2025).
[4] *Id.*

7. UPenn's spokesperson stated "Please know that we are actively and quickly investigating and taking immediate steps to stop these emails from being sent… Our IT team at Penn GSE and the University's IT team and Crisis Response Teams are working as quickly as they can."[5]

8. Upon information and belief, the types of PII accessed and/or acquired in the Data Breach included highly sensitive information such as: name, demographic information (such as address, city, state, and zip code), and Social Security numbers (collectively, "Private Information").

9. Upon information and belief, due to Defendant's negligence, cybercriminals have accessed and obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals including Plaintiff.

10. UPenn breached its duty and betrayed the trust of Plaintiff and Class members by failing to properly safeguard and protect their personal information, thus enabling cybercriminals to access, acquire, appropriate, compromise, disclose, encumber, exfiltrate, steal, misuse, and/or view it.

11. Now, and for the rest of their lives, Plaintiff and the Class Members will have to deal with the danger of identity thieves possessing and misusing their Private Information. Even those Class Members who have yet to experience identity theft have to spend time responding to the Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and

[5] *See* https://www.thedp.com/article/2025/10/penn-gse-emails-we-got-hacked-subject-security-breach (last visited Oct. 31, 2025).

Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their Private Information, loss of privacy, and/or additional damages as described below.

12. In sum, Plaintiff and the Class will face an imminent risk of fraud and identity theft for the rest of their lives because: (i) UPenn failed to protect Plaintiff's and the Class's Private Information, allowing a large and preventable Data Breach to occur; (ii) the cybercriminals who perpetrated the Breach accessed Private Information that they will sell on the dark web (if they have not already) because that is the *modus operandi* of cybercriminals who perpetrate breaches such as this; and (iii) Plaintiff and Class members are at immediate risk of experiencing misuse of their PII.

13. Plaintiff brings this action individually and on behalf of the Class, seeking compensatory damages, punitive damages, nominal damages, restitution, and injunctive and declaratory relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

II. THE PARTIES

14. Plaintiff **Christopher F. Kelly** is an individual domiciled in Chicago, Illinois. Plaintiff is an alum of UPenn. Plaintiff received the email sent out by the unknown actors that perpetrated the Data Breach. Upon information and belief, Plaintiff is a victim of the Data Breach.

15. Defendant **University of Pennsylvania** is a private educational institution with its principal place of business in Philadelphia, Pennsylvania.

III. JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than one hundred putative Class Members, and minimal diversity exists because many putative Class Members are citizens of a different state than Defendant.

17. This Court has personal jurisdiction over Defendant because Defendant is registered to do business in the State of Pennsylvania; has its principal place of business in this District; conducts substantial business in this District through its headquarters, offices, and affiliates; engaged in the conduct at issue here in this District; and/or otherwise has substantial contacts with this District and purposely availed itself to the Courts in this District.

18. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District. Upon information and belief, the Data Breach giving rise to this lawsuit occurred in this District.

IV. FACTUAL ALLEGATIONS

A. Defendant and its Collection of Plaintiff's and the Class's PII.

19. UPenn is a private institution of higher learning located within the City and County of Philadelphia, Pennsylvania. UPenn offers academic degrees in a variety of disciplines.

20. As part of its business, and in order to gain profits, UPenn obtained and stored

the personal information of its students, applicants, and faculty, including the personal information of Plaintiff and Class members.

21. It is estimated that UPenn's annual revenue is over $15 billion per year.[6] In other words, UPenn could have afforded to implement adequate data security prior to the Breach but deliberately chose not to.

22. UPenn obtains, collects, uses, and derives a benefit from the Private Information of Plaintiff's and Class Members. UPenn uses the Private Information it collects to provide services, making a profit therefrom. UPenn would not be able to obtain revenue if not for the acceptance and use of Plaintiff's and the Class's Private Information.

23. By collecting Plaintiff's and the Class's Private Information, UPenn assumed legal and equitable duties to Plaintiff and the Class to protect and safeguard their Private Information from unauthorized access and intrusion.

24. UPenn recognized it had a duty to use reasonable measures to protect the Private Information that it collected and maintained.

25. UPenn failed to adopt reasonable and appropriate data security practices and procedures including administrative, physical security, and technical controls to safeguard Plaintiff's and the Class's Private Information.

[6] UPenn Annual Financial Report (2023-2024) https://www.finance.upenn.edu/wp-content/uploads/Penn-Division-of-Finance-FY24-Annual-Report.pdf (last visited Oct. 31, 2025).

26. As a result, Plaintiff's and Class Members' Private Information was accessed and/or stolen from UPenn's inadequately secured email accounts and/or network in a large and preventable Data Breach.

B. UPenn's Data Breach.

27. On or around October 31, 2025, due to UPenn's failure to maintain an adequate security system, an unknown third actor gained access to UPenn's systems and acquired certain files and information, including Plaintiff's and Class Members' PII.

28. Upon information and belief, the targeted cyberattack was expressly designed to gain access to and exfiltrate private and confidential information, including (among other things) the PII of Plaintiff and the Class members. Upon information and belief, UPenn failed to pay a ransom to the unknown actors and the unknown actors have threatened to lead the PII of Plaintiff and Class members.

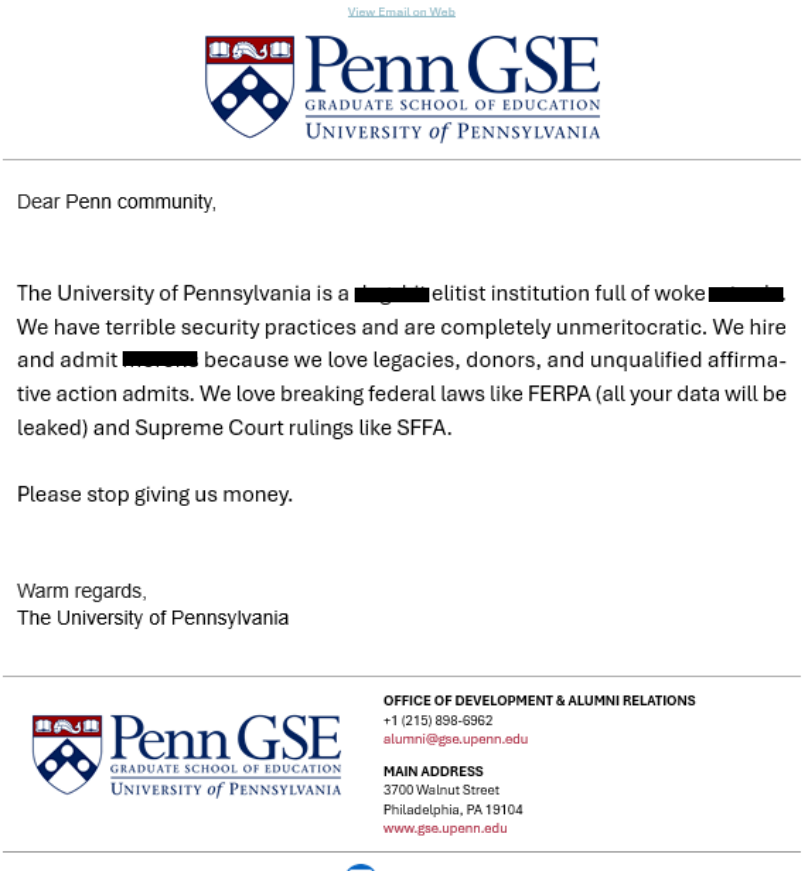
29. Upon information and belief, the types of PII accessed and/or acquired in the Data Breach included highly sensitive information such as: name, demographic information (such as address, city, state, and zip code), and Social Security numbers (collectively, "Private Information").

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

31. As part of the Data Breach, a series of mass emails were sent to students,

faculty, alumni, and parents from accounts linked to the Graduate School of Education.[7] In the series of emails, the unknown actors stated "all your data will be leaked."[8] Other Penn affiliates have received the email multiple times from different senders with official "@upenn.edu" email addresses.[9]

32. Upon information and belief, the following email was sent by the unknown actors that perpetrated the Data Breach to UPenn students, faculty, and alumni:[10]



View Email on Web

Penn GSE
GRADUATE SCHOOL OF EDUCATION
UNIVERSITY of PENNSYLVANIA

Dear Penn community,

The University of Pennsylvania is a [redacted] elitist institution full of woke [redacted]. We have terrible security practices and are completely unmeritocratic. We hire and admit [redacted] because we love legacies, donors, and unqualified affirmative action admits. We love breaking federal laws like FERPA (all your data will be leaked) and Supreme Court rulings like SFFA.

Please stop giving us money.

Warm regards,
The University of Pennsylvania

Penn GSE
GRADUATE SCHOOL OF EDUCATION
UNIVERSITY of PENNSYLVANIA

OFFICE OF DEVELOPMENT & ALUMNI RELATIONS
+1 (215) 898-6962
alumni@gse.upenn.edu

MAIN ADDRESS
3700 Walnut Street
Philadelphia, PA 19104
www.gse.upenn.edu

[7] *See* https://www.thedp.com/article/2025/10/penn-gse-emails-we-got-hacked-subject-security-breach (last visited Oct. 31, 2025).
[8] *See* https://techcrunch.com/2025/10/31/hackers-threaten-to-leak-data-after-breaching-university-of-pennsylvania-to-send-mass-emails/ (last visited Oct. 31, 2025).
[9] *Id.*
[10] Inappropriate language in the above email has been redacted.

33. The unencrypted PII of Plaintiff and Class Members may end up for sale on the dark web or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Upon information and belief, unauthorized individuals can easily access the PII of Plaintiff and Class members.

34. UPenn was negligent and did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing the exposure of PII for Plaintiff and Class Members.

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

36. UPenn breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Upon information and belief, UPenn's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect students' and faculty's PII;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

f. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

g. Failing to adhere to industry standards for cybersecurity as discussed above; and

h. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information

37. UPenn negligently and unlawfully failed to safeguard Plaintiff's and Class Members' PII by allowing cyberthieves to access UPenn's computer network and systems which contained unsecured and unencrypted PII.

38. Accordingly, Plaintiff and Class members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendants.

39. UPenn's actions represent a flagrant disregard of the rights of Plaintiff and the Class, both as to privacy and property.

C. Cybercriminals Have Used and Will Continue to Use Plaintiff's and the Class's PII to Defraud Them.

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

41. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[11]

42. For example, with the PII stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[12] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and the Class Members.

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

> **Social Security number.** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refunds, employment – even

[11] *Facts + Statistics: Identity Theft and Cybercrime*, INSURANCE INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[12] *See, e.g.*, Christine DiGangi, *What Can You Do with a Stolen Social Security Number*, CREDIT.COM (June 29, 2020), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

> using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your life in so many ways.[13]

44. PII is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[14]

45. This was a financially motivated Breach, as the only reason the cybercriminals go through the trouble of running targeted cyberattacks against companies like UPenn is to get ransom money and/or information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein.

46. Indeed, a social security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[15]

47. "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[16]

---

[13] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/ (emphasis added).

[14] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, available at https://www.gao.gov/products/gao-07-737.

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

[16] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

48. These risks are both certainly impending and substantial. As the Federal Trade Commission ("FTC") has reported, if hackers get access to PII, ***they will use it***.[17]

49. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information ***may continue for years***. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[18]

50. For instance, with a stolen social security number, which is part of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[19]

51. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[20]

52. The full scope of the harm has yet to be realized. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is

---

[17] Ari Lazarus, *How fast will identity thieves use stolen info?*, MILITARY CONSUMER (May 24, 2017), https://www.militaryconsumer.gov/blog/how-fast-will-identity-thieves-use-stolen-info.

[18] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,* GAO (July 5, 2007), available at https://www.gao.gov/products/gao-07-737.

[19] *See, e.g.*, Christine DiGangi, *What Can You Do with a Stolen Social Security Number*, CREDIT.COM (June 29, 2020), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[20] *Guide for Assisting Identity Theft Victims*, FEDERAL TRADE COMMISSION (Sept. 2013), *available at* https://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf.

stolen and when it is used.

53. Plaintiff and Class Members will need to pay for their own identity theft protection and credit monitoring for the rest of their lives due to UPenn's gross negligence.

54. Furthermore, identity monitoring only alerts someone to the fact that they have already been the victim of identity theft (*i.e.*, fraudulent acquisition and use of another person's PII)—it does not prevent identity theft.[21] Nor can an identity monitoring service remove personal information from the dark web.[22]

55. "The people who trade in stolen personal information [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."[23]

56. As a direct and proximate result of the Data Breach, Plaintiff and the Class have been damaged and have been placed at an imminent, immediate, and continuing increased risk of harm from continued fraud and identity theft. Plaintiff and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts,

[21] *See, e.g.*, Kayleigh Kulp, *Credit Monitoring Services May Not Be Worth the Cost*, CNBC (Nov. 30, 2017, 9:00 AM), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html.
[22] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know.
[23] *Id.*

and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

57. Even more seriously is the identity restoration that Plaintiff and other Class Members must go through, which can include spending countless hours filing police reports, filling out IRS forms, Federal Trade Commission checklists, Department of Motor Vehicle driver's license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiff and the Class must take.

58. Plaintiff and the Class have or will experience the following concrete and particularized harms for which they are entitled to compensation, including:

a. Actual identity theft;

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

c. Improper disclosure of their PII;

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

e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their PII;

f. Ascertainable losses in the form of time taken to respond to identity theft and attempt to restore identity, including lost opportunities and lost wages from uncompensated time off from work;

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

h. Ascertainable losses in the form of deprivation of the value of Plaintiff's and Class Members' Private Information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their PII; and/or

k. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

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

60. Plaintiff and Class Members also have an interest in ensuring that their Private Information that was provided to UPenn is removed from all UPenn servers, systems, and files if no longer needed by UPenn.

61. UPenn also admitted its current data security measures were not adequate because it stated, "Please know that we are actively and quickly investigating and taking

immediate steps to stop these emails from being sent… Our IT team at Penn GSE and the University's IT team and Crisis Response Teams are working as quickly as they can."[24]

62. These enhanced protections should have been in place before the Data Breach.

63. At UPenn's suggestion, Plaintiff and the Class are desperately trying to mitigate the damage that UPenn has caused them.

64. Given the kind of Private Information UPenn made accessible to hackers, however, Plaintiff and the Class are certain to incur additional damages. Because identity thieves have their PII, Plaintiff and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with a new number.[25]

65. None of this should have happened because the Data Breach was entirely preventable.

D. Defendant was Aware of the Risk of Cyberattacks.

66. Data security breaches have dominated the headlines for the last two decades. And it doesn't take an IT industry expert to know it. The general public can tell you the

[24] *See* https://www.thedp.com/article/2025/10/penn-gse-emails-we-got-hacked-subject-security-breach (last visited Oct. 31, 2025).
[25] *What happens if I change my Social Security number*, LEXINGTON LAW (Aug. 10, 2022), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.

names of some of the biggest cybersecurity breaches: Target,[26] Yahoo,[27] Marriott International,[28] Chipotle, Chili's, Arby's,[29] and others.[30]

67. The number of data breach victims has surpassed 1 billion for the first half of 2024, according to the Identity Theft Resource Center.[31]

68. UPenn should certainly have been aware, and indeed was aware, that it was at risk of a data breach that could expose the PII that it collected and maintained.

69. UPenn was clearly aware of the risks it was taking and the harm that could result from inadequate data security but threw caution to the wind.

E. UPenn Failed to Comply with FTC Guidelines and Industry Standards

70. Data breaches are preventable.[32] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that

---

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

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

[28] Patrick Nohe, *The Marriot Data Breach: Full Autopsy*, THE SSL STORE: HASHEDOUT (Mar. 22, 2019), https://www.thesslstore.com/blog/autopsying-the-marriott-data-breach-this-is-why-insurance-matters/ (last visited Oct. 9, 2023).

[29] Alfred Ng, *FBI Nabs Alleged Hackers in Theft of 15M Credit Cards from Chipotle, Others*, CNET (Aug. 1, 2018, 12:58 PM), https://www.cnet.com/news/fbi-nabs-alleged-hackers-in-theft-of-15m-credit-cards-from-chipotle-others/?ftag=CMG-01-10aaa1b.

[30] *See, e.g.*, Michael Hill and Dan Swinhoe, *The 15 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Nov. 8, 2022), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[31] https://www.usatoday.com/story/money/2024/07/18/data-breach-what-to-do/74441060007/.

[32] 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.

occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[33] he added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[34]

71. "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*."[35]

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

73. The FTC has published guidelines that establish reasonable data security practices for businesses.

74. 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.[36]

75. 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

[33] *Id.* at 17.
[34] *Id.* at 28.
[35] *Id.*
[36] *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.

vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems.

76. 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.

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

78. Upon information and belief, UPenn 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.

79. 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."[37]

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

80. 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.
- 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.[38]

81. 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)….

[38] *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….[39]

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

82. 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**
  - 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].[40]

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

84. Specifically, among other failures, UPenn had far too much confidential unencrypted information held on its systems. Such PII should have been segregated into an encrypted system.[41]

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

86. The FTC, among others, has repeatedly emphasized the importance of disposing unnecessary PII, 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

[40] *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/.
[41] *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.

of it. If it's not on your system, it can't be stolen by hackers."[42] UPenn, rather than following this basic standard of care, kept thousands of individuals' unencrypted PII indefinitely.

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

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

F. Plaintiff's Christopher Kelly's Experience

89. Plaintiff Kelly is an UPenn alum. Upon information and belief, Plaintiff is a victim of the data breach.

90. Plaintiff received the email sent by the unknown actors that perpetrated the Data Breach (as alleged in paragraph 32 above).

91. In order to receive services from Defendant, Plaintiff provided Defendant with his PII, including his name, date of birth, Social Security number, email address, physical address, and phone number. Defendant accepted and stored this PII in the regular course of business.

92. Plaintiff entrusted his PII to Defendant with the reasonable expectation and mutual understanding that Defendant would keep his PII secure from unauthorized access.

93. By soliciting and accepting Plaintiff's PII, Defendant agreed to safeguard

[42] *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.

and protect it from unauthorized access and delete it after a reasonable time.

94. Plaintiff is very careful about sharing his sensitive PII. Plaintiff stores any documents containing his PII in a safe and secure location. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff would not have entrusted his PII to Defendant had he known of Defendant's lax data security policies.

95. Upon information and belief, Defendant was in possession of Plaintiff's PII before, during, and after the Data Breach.

96. Plaintiff reasonably understood and expected that Defendant would safeguard his PII and timely and adequately notify him in the event of a data breach.

97. Plaintiff would not have allowed Defendant, or anyone in Defendant's position, to maintain his PII if he believed that Defendant would fail to implement reasonable and industry standard practices to safeguard his PII from unauthorized access and exfiltration.

98. Plaintiff is very concerned about theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

99. As a result of the Data Breach, upon information and belief, Plaintiff's PII has been accessed and/or acquired by an unauthorized actor. Upon information and belief, the confidentiality of Plaintiff's PII has been irreparably harmed. For the rest of his life, Plaintiff will have to worry about when and how his PII may be shared or used to his detriment.

100. As a result of the Data Breach, Plaintiff has spent hours dealing with the

consequences of the Data Breach, which includes time spent verifying the legitimacy of the Data Breach, self-monitoring his accounts, reviewing credit reports, and mitigating fraud and identity theft. This time has been lost forever and cannot be recaptured.

101. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by Defendant's delay in noticing him of the fact that his PII was accessed and/or acquired by criminals as a result of the Data Breach.

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

103. Upon information and belief, Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and experiences fear and anxiety and increased concern for the loss of his privacy.

104. As a result of the Data Breach, Plaintiff has received an increased amount of spam emails, spam texts, and spam phone calls, evidencing that cybercriminals are in possession of his sensitive PII.

105. Upon information and belief, as a direct and traceable result of the Data Breach, Plaintiff suffered actual injury and damages after his PII was compromised in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts and/or credit reports for fraudulent activity and researching the Data Breach; (b) loss of privacy due to his PII being accessed and/or stolen by cybercriminals; (c) loss of the benefit of the bargain because Defendants did not adequately protect his PII; (d)

emotional distress because identity thieves now possess his PII; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PII has likely been stolen and published on the dark web; (f) diminution in the value of his PII, a form of intangible property that Defendant obtained from Plaintiff; and (g) other economic and non-economic harm.

106. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

107. Plaintiff 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 PII stolen in the Data Breach.

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

V. CLASS ACTION ALLEGATIONS

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

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

> **All persons whose PII was compromised in the Data Breach, including all individuals who were sent a Notice Letter after the Data Breach.**

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

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

113. Plaintiff anticipates the issuance of notice setting forth the subject and nature of the instant action to the proposed Class. Upon information and belief, Defendant's own business records or electronic media can be utilized for the notice process.

114. The proposed Class meets the requirements of Federal Rule of Civil Procedure 23.

115. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. Upon information and belief, thousands of UPenn students, faculty, and alumni have been affected by the Data Breach.

116. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through UPenn's uniform misconduct. UPenn's inadequate data security gave rise to Plaintiff's claims and are identical to those that give rise to the claims of every other Class member because Plaintiff and each member of the Class had their sensitive PII compromised in the same way by the same conduct of UPenn.

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

118. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the Class individually to effectively redress UPenn's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

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

a. Whether Defendant engaged in the wrongful conduct alleged herein;

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

c. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their PII, and whether it breached this duty;

d. Whether UPenn breached its duties to Plaintiff and the Class;

e. Whether UPenn failed to provide adequate cyber security;

f. Whether UPenn knew or should have known that its computer and network security systems were vulnerable to cyber-attacks;

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

h. Whether UPenn was negligent in permitting unencrypted PII off vast numbers of individuals to be stored within its network;

i. Whether UPenn was negligent in failing to adhere to reasonable retention policies, thereby greatly increasing the size of the Data Breach;

j. Whether UPenn breached implied contractual duties to Plaintiff and the Class to use reasonable care in protecting their PII;

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

l. Whether UPenn continues to breach duties to Plaintiff and the Class;

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

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

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

VI. CAUSES OF ACTION

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

120. Plaintiff incorporates paragraphs 1–106 as though fully set forth herein.

121. UPenn solicited, gathered, and stored the Private Information of Plaintiff and Class Members.

122. Upon accepting and storing the Private Information of Plaintiff and Class Members on its computer systems, email accounts, and networks, Defendant undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information of Plaintiff and the Class from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

123. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if the Private Information was wrongfully disclosed. Plaintiff and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class Members

had no ability to protect their Private Information that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiff and the Class.

124. Because of this special relationship, Defendant required Plaintiff and Class Members to provide their Private Information, including names, Social Security numbers, and other Private Information.

125. Implied in these exchanges was a promise by Defendant to ensure that the Private Information of Plaintiff and Class Members in its possession was only used for the provided purpose and that Defendant would destroy any Private Information that it was not required to maintain.

126. As part of this special relationship, Defendant had a duty to perform with skill, care, and reasonable expedience and faithfulness.

127. Through Defendant's acts and omissions, including Defendant's failure to provide adequate data security, its failure to protect Plaintiff's and Class Members' Private Information from being foreseeably accessed, and its improper retention of Private Information it was not required to maintain, Defendant negligently failed to observe and perform its duty.

128. Plaintiff and Class Members did not receive the benefit of the bargain with Defendant, because providing their Private Information was in exchange for Defendant's implied agreement to secure and keep it safe and to delete it once no longer required.

129. Defendant was aware of the fact that cybercriminals routinely target companies and corporations through cyberattacks in an attempt to steal customer and

employee Private Information. In other words, Defendant knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures.

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

131. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

132. Defendant had duties to protect and safeguard the Private Information of Plaintiff and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive Private Information. Additional duties that Defendant owed Plaintiff, and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant's networks, systems, email accounts, protocols, policies, procedures and practices to ensure that Plaintiff's and Class Members' Private Information was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiff's and Class Members' Private Information in its possession by using reasonable and adequate security procedures and systems;

c. To implement processes to quickly detect a data breach, security incident, or intrusion involving its networks, email accounts, and servers; and

d. To promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their Private Information.

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

134. Plaintiff's injuries and damages, as described herein, are a reasonably certain consequence of Defendant's negligence and breach of its duties.

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

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

b. Failing to protect the Private Information in its possession using reasonable and adequate security procedures and systems;

c. Failing to consistently enforce security policies aimed at protecting Plaintiff and the Class's Private Information;

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

e. Failing to promptly notify Plaintiff and Class Members of the Data Breach that affected their Private Information.

136. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent considering the foreseeable risks and known threats.

137. As a direct and proximate result of Defendant's negligent conduct, including but not limited to its failure to implement and maintain reasonable data security practices and procedures as described above, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

138. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Private Information of Plaintiff and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiff and Class Members while it was within Defendant's possession and control.

139. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps to securing their Private Information and mitigating damages.

140. Plaintiff and Class Members could have taken actions earlier had they been timely notified of the Data Breach.

141. Plaintiff and Class Members could have enrolled in credit monitoring, could have instituted credit freezes, and could have changed their passwords, among other things, had they been alerted to the Data Breach more quickly.

142. Plaintiff and Class Members have suffered harm from the delay in notifying them of the Data Breach.

143. As a direct and proximate cause of Defendant's conduct, including but not limited to its failure to implement and maintain reasonable security practices and procedures, Plaintiff and Class Members have suffered, as Plaintiff have, and/or will suffer injury and damages, including but not limited to: (i) the loss of the opportunity to determine for themselves how their Private Information is used; (ii) the publication and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information, including the need for substantial credit monitoring and identity protection services for an extended period of time; (iv) 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 tax fraud and identity theft; (v) costs associated with placing freezes on credit reports and password protections; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their Private Information, which remains in Defendant's

possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of employees in its continued possession; and, (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Private Information for the rest of their lives. Thus, Plaintiff and the Class are entitled to damages in an amount to be proven at trial.

144. The damages Plaintiff and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's negligent conduct.

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

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

146. Plaintiff incorporates paragraphs 1–106 as though fully set forth herein.

147. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant had a duty to Plaintiff and the Class to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and the Class.

148. The FTC Act prohibits "unfair practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

149. Defendant gathered and stored the Private Information of Plaintiff and the Class as part of their business which affects commerce.

150. Defendant violated the FTC Act by failing to use reasonable measures to protect the Private Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

151. Defendant breached its duties to Plaintiff and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiff's and Class Members' Private Information, and by failing to provide prompt notice without reasonable delay.

152. Defendant's multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

153. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

154. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against.

155. Defendant breached its duties to Plaintiff and the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class's Private Information.

156. Defendant breached its duties to Plaintiff and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiff and the Class.

157. Defendant's violations of the FTC Act constitute negligence *per se*.

158. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

159. The injury and harm that Plaintiff and Class Members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

160. Plaintiff and the Class have suffered injury and are entitled to damages in amounts to be proven at trial.

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

161. Plaintiff incorporates paragraphs 1–106 as though fully set forth herein.

162. Plaintiff and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their information had been breached and compromised.

163. Plaintiff and Class Members were required to deliver, and did deliver, their PII to Defendant as part of the process of obtaining educational services provided by Defendant. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

164. Defendant solicited, offered, and invited Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

165. Defendant accepted possession of Plaintiff's and Class Members' PII for the

purpose of providing services to Plaintiff and Class Members.

166. When Plaintiff and Class Members paid money and provided their PII to Defendant, either directly or indirectly, in the exchange for goods and services, they entered into implied contracts with Defendant, and intended and understood that Private Information would be adequately safeguarded as part of that service.

167. Plaintiff and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such PII and to timely and accurately notify Plaintiff and Class Members that their information had been breached and compromised.

168. In accepting such information and payment for services, Plaintiff and the other Class Members entered into an implied contract with Defendant whereby Defendant became obligated to reasonably safeguard Plaintiff's and the other Class Members' PII.

169. In delivering their PII to Defendant and paying for higher education services, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard the data as part of that service.

170. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under FTC or other state of federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

171. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to PII also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of its agents is

restricted and limited to achieve an authorized educational purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6) multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

172. Plaintiff and Class Members would not have entrusted their PII to Defendants in the absence of such an implied contract.

173. Had Defendant disclosed to Plaintiff and Class Members that it did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and the other Class Members would not have provided their PII to Defendant.

174. Defendant recognized that Plaintiff's and Class Members' PII is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

175. Plaintiff and the other Class Members fully performed their obligations under the implied contracts with Defendants.

176. Defendant breached the implied contract with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their PII as described herein.

177. As a direct and proximate result of Defendants' conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial, or alternatively, nominal damages.

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

178. Plaintiff incorporates paragraphs 1–106 as though fully set forth herein.

179. Plaintiff alleges this claim in the alternative where necessary.

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

181. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiff and Class Members.

182. As such, a portion of the payments made for the benefit of or on behalf of Plaintiff and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

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

184. Defendant acquired the Private Information through inequitable means as it failed to disclose the inadequate data security practices previously alleged. If Plaintiff and Class Members had known that Defendant would not fund adequate data security practices, procedures, and protocols to sufficiently monitor, supervise, and secure their Private

Information, they would not have entrusted their Private Information to Defendant.

185. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to their own benefit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

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

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

188. As a direct and proximate result of Defendant's conduct, Plaintiff and other Class Members, have suffered actual harm in the form of experiencing specific acts of fraudulent activity and other attempts of fraud that required Plaintiff' efforts to prevent from succeeding.

189. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class are entitled to restitution and disgorgement of profits, benefits, and other compensation obtained by Defendant and all other relief allowed by law.

FIFTH CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiff and the Class)

190. Plaintiff incorporates paragraphs 1–106 as though fully set forth herein.

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

192. As previously alleged, Plaintiff and members of the Class are entered into implied contracts with Defendant, which contracts required Defendant to provide adequate security for the Private Information collected from Plaintiff and the Class.

193. Defendant owed and still owes a duty of care to Plaintiff and Class Members that require it to adequately secure Plaintiff's and Class Members' Private Information.

194. Upon reason and belief, Defendant still possesses the Private Information of Plaintiff and the Class Members.

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

196. Since the Data Breach, Defendant has not yet announced any specific changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and go undetected and, thereby, prevent further attacks.

197. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class. In fact, now that Defendant's insufficient data security is known to hackers, the Private Information in Defendant's possession is even more vulnerable to cyberattack.

198. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and the members of the Class. Further, Plaintiff and the members of the Class are at risk of

additional or further harm due to the exposure of their Private Information and Defendant's failure to address the security failings that led to such exposure.

199. There is no reason to believe that Defendant's security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

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

a. Ordering that Defendant engage 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;

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

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

d. Ordering that Defendant segment employee data by, among other things, creating firewalls and access controls so that if one area of Defendant's

systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant purge, delete, and destroy, in a reasonably secure manner, customer data not necessary for their provisions of services;

f. Ordering that Defendant conduct regular database scanning and security checks; and

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

VII. PRAYER FOR RELIEF

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

a. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff are proper representatives of the Class requested herein;

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

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

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

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

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

VIII. DEMAND FOR JURY TRIAL

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

Dated: November 3, 2025

Respectfully submitted,

/s/ Randi Kassan
Randi Kassan (PBN 323790)
MILBERG, PLLC
100 Garden City Plaza, Suite 408
Garden City, NY 11530
Tel: (516) 741-5600
rkassan@milberg.com

William B. Federman (*pro hac vice* forthcoming)
Jessica A. Wilkes (*pro hac vice* forthcoming)
Jonathan Herrera (*pro hac vice* forthcoming)
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
Telephone: (405) 235-1560
wbf@federmanlaw.com

jaw@federmanlaw.com
jjh@federmanlaw.com

Counsel for Plaintiff and Proposed Lead Counsel for the Class