Robert T. Mills (Arizona Bar #018853)
Sean A. Woods (Arizona Bar #028930)
MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, Arizona 85014
Telephone 480.999.4556
docket@millsandwoods.com
swoods@millsandwoods.com

Tyler J. Bean (*Pro Hac Vice Anticipated*)
SIRI & GLIMSTAD LLP
745 Fifth Ave., Ste. 500
New York, NY 10151
Tel: (212) 532-1091
tbean@sirillp.com

Attorneys for Plaintiffs and the Putative Class

UNITED STATES DISTRICT COURT

DISTRICT OF ARIZONA

Melissa Neblock and Antonyo Wyche, on behalf of themselves and all others similarly situated, Plaintiffs, vs. The University of Phoenix, Inc., Defendant.	Case No.: **CLASS ACTION COMPLAINT**

Plaintiffs Melissa Neblock and Antonyo Wyche ("Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against The University of Phoenix, Inc. ("University of Phoenix" or "Defendant") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by Plaintiffs' counsel and review of public documents as to all other matters:

///

///

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

I. INTRODUCTION

1. Plaintiffs bring this class action against University of Phoenix for its failure to properly secure and safeguard Plaintiffs' and other similarly situated person's name and Social Security number (the "Private Information") from hackers.

2. University of Phoenix, based in Phoenix, Arizona, is an online institution of higher education that serves thousands of students nationwide.

3. On or about December 22, 2025, University of Phoenix filed official notice of a hacking incident with the Office of the Maine Attorney General.[1]

4. On or about the same date, University of Phoenix also sent out data breach letters to individuals whose information was compromised as a result of the hacking incident (the "Notice").

5. Based on the Notice filed by the company, on November 21, 2025, University of Phoenix learned that its vendor experienced unusual activity on their computer systems. In response, the University of Phoenix launched an investigation. The University of Phoenix investigation revealed that between August 13, 2025, and August 22, 2025, an unauthorized party had access to certain company files containing the Private Information that University of Phoenix stored on behalf of its students (the "Data Breach").

6. Plaintiffs and "Class Members" (defined below) were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

[1] *See* https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/422db005-448f-4772-afc6-07dabfa169a8.html (last visited Jan. 7, 2026).

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

7. The Private Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves, including but not limited to, names and Social Security numbers that University of Phoenix collected and maintained on behalf of its students.

8. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

9. There has been no assurance offered by University of Phoenix that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach in the future.

10. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

11. Plaintiffs bring this class action lawsuit to address University of Phoenix's inadequate safeguarding of Class Members' Private Information that it collected and maintained on behalf of its students, and its failure to provide adequate notice to its students regarding the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

12. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to University of Phoenix, and thus University of Phoenix was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

13. Upon information and belief, University of Phoenix and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had University of Phoenix properly monitored the networks, it would have discovered the Breach sooner.

14. Plaintiffs' and Class Members' identities are now at risk because of University of Phoenix's negligent conduct as the Private Information that University of Phoenix collected and maintained on behalf of its students is now in the hands of data thieves and other unauthorized third parties.

15. Plaintiffs seek to remedy these harms on behalf of themselves, and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

///

///

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

II. PARTIES

16. Plaintiff Melissa Neblock is, and at all times mentioned herein was, an individual citizen of the State of Illinois.

17. Plaintiff Antonyo Wyche is, and at all times mentioned herein was, an individual citizen of the State of Georgia.

18. Defendant The University of Phoenix, Inc. is an online institution of higher education with its principal place of business at 4035 South Riverpoint Parkway, Phoenix, AZ 85040.

III. JURISDICTION AND VENUE

19. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from University of Phoenix. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

20. This Court has jurisdiction over University of Phoenix because University of Phoenix operates in and/or is incorporated in this District.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and University of Phoenix has harmed Class Members residing in this District.

///

///

///

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

IV. FACTUAL ALLEGATIONS

A. *University of Phoenix's Business and Collection of Plaintiffs' and Class Members' Private Information.*

22. University of Phoenix is an online institution of higher education. Founded in 1976, University of Phoenix offers a wide variety of courses ranging from business, technology, healthcare, education and more, serving thousands of students nationwide. University of Phoenix employs more than 7,000 people and generates approximately $2.1 billion in annual revenue.

23. As a condition of receiving educational services, University of Phoenix requires that its students entrust it with highly sensitive personal information. In the ordinary course of receiving educational services from University of Phoenix's students, Plaintiffs and Class Members were required to provide their Private Information to Defendant.

24. In its "Notice of Data Security Incident" Defendant states "The university of Phoenix, Inc. takes the privacy and security of all information within its possession very seriously."[2] In its privacy policy, Defendant also informs its students that "[w]e have implemented security measures to protect against the loss, misuse, and alteration of the Personal Information under our control."[3]

25. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, University of Phoenix assumed legal and equitable

[2] *See* https://www.phoenix.edu/copyright-legal/privacy-policy.html#disclosure (last visited Jan. 7, 2026).
[3] *Id.*

duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

B. *The Data Breach and University of Phoenix's Inadequate Notice to Plaintiffs and Class Members*

26. According to Defendant's Notice, it learned of unauthorized access to its vendor's computer systems on November 21, 2025, with such unauthorized access having taken place between August 13, 2025, and August 22, 2025.

27. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including names and Social Security numbers, relating to its students.

28. University of Phoenix delivered Data Breach Notification Letters to Plaintiffs and Class Members, alerting them that their highly sensitive Private Information had been exposed in a "Data Security Incident."

29. Omitted from the Notice are crucial details like 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 critical facts have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information is protected.

30. Thus, University of Phoenix's purported disclosure amounts to no real disclosure at all, as it fails to inform Plaintiffs and Class Members of the Data Breach's critical facts with any degree of specificity. Without these details, Plaintiffs' and Class Members' ability to mitigate the harms resulting from the Data Breach was and is severely diminished.

Mills + Woods Law, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

31. In addition, the Notice offers no substantive steps to help victims like Plaintiffs and Class Members to protect themselves other than providing one year of credit monitoring – an offer that is woefully inadequate considering the lifelong increased risk of fraud and identity theft Plaintiffs and Class Members now face as a result of the Data Breach.

32. University of Phoenix had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

33. Plaintiffs and Class Members provided their Private Information to University of Phoenix, with the reasonable expectation and mutual understanding that University of Phoenix would comply with its obligations to keep such information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

34. University of Phoenix's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

35. University of Phoenix knew or should have known that its students' electronic records would be targeted by cybercriminals.

C. *The University of Phoenix Knew or Should Have Known of the Risk of a Cyber Attack Because Businesses in Possession of Private Information are Particularly Susceptible.*

36. University of Phoenix's negligence, including its gross negligence, in failing to safeguard Plaintiffs' and Class Members' Private Information is particularly stark,

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

considering the highly public increase of cybercrime similar to the hacking incident that resulted in the Data Breach.

37. Data thieves regularly target entities like University of Phoenix due to the highly sensitive information they maintain. University of Phoenix knew and understood that Plaintiffs' and Class Members' Private Information is valuable and highly sought after by criminal parties who seek to illegally monetize it through unauthorized access.

38. According to the Identity Theft Resource Center's 2023 Data Breach Report, the overall number of publicly reported data compromises in 2023 increased more than 72-percent over the previous high-water mark and 78-percent over 2022.[4]

39. Moreover, third-party vendors like University of Phoenix are an especially common target for hackers. In 2023, approximately 29-percent of all data breaches resulted from a "third-party attack vector" and, as much data breach reporting does not specify the attack vector, "the actual percentage of breaches occurring via third parties was probably higher."[5]

40. Despite the prevalence of public announcements of data breach and data security compromises, University of Phoenix failed to take appropriate steps to protect Plaintiffs' and Class Members' Private Information from being compromised in this Data

[4] *2023 Annual Data Breach Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2024), *available online at*: https://www.idtheftcenter.org/wp-content/uploads/2024/01/ITRC_2023-Annual-Data-Breach-Report.pdf (last visited on Jan. 7, 2026).

[5] *Global Third-Party Cybersecurity Breaches*, SECURITYSCORECARD (2024), *available online at*: https://securityscorecard.com/reports/third-party-cyber-risk/ (last visited on Jan. 7, 2026).

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

Breach.

41. As a national service provider in possession of millions of customers' Private Information, University of Phoenix knew, or should have known, the importance of safeguarding the Private Information entrusted to it by Plaintiffs and Class Members and of the foreseeable consequences they would suffer if University of Phoenix's data security systems were breached. Such consequences include the significant costs imposed on Plaintiffs and Class Members due to the unauthorized exposure of their Private Information to criminal actors. Nevertheless, University of Phoenix failed to take adequate cybersecurity measures to prevent the Data Breach or the foreseeable injuries it caused.

42. Given the nature of the Data Breach, it was foreseeable that Plaintiffs' and Class Members' Private Information compromised therein would be targeted by hackers and cybercriminals, for use in variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiffs' and Class Members' Private Information can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiffs' and Class Members' names.

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

44. Plaintiffs and Class Members were the foreseeable and probable victims of University of Phoenix's inadequate security practices and procedures. University of Phoenix knew or should have known of the inherent risks in collecting and storing the

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

Private Information and the critical importance of providing adequate security for that data, particularly due to the highly public trend of data breach incidents in recent years.

D. *University of Phoenix Failed to Comply with FTC Guidelines.*

45. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

46. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[6] The guidelines note that businesses should protect the personal customer 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 to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting

[6] *Protecting Personal Information: A Guide for Business,* FEDERAL TRADE COMMISSION (October 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited on Jan. 7, 2026).

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

47. The FTC further recommends that companies not maintain personally identifiable information ("PII") longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, and monitor their networks for suspicious activity.

48. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45 *et seq*. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

49. Such FTC enforcement actions include those against businesses that fail to adequately protect customer data, like University of Phoenix here. *See, e.g.*, *In the Matter of LabMD, Inc*., 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

50. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like University of Phoenix of failing to use reasonable measures to protect Private Information they collect and maintain from consumers. The FTC

publications and orders described above also form part of the basis of University of Phoenix's duty in this regard.

51. The FTC has also recognized that personal data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis and profit."[7]

52. As evidenced by the Data Breach, University of Phoenix failed to properly implement basic data security practices. University of Phoenix's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

53. University of Phoenix was at all times fully aware of its obligation to protect the Private Information of its students yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

///

///

[7] FTC Commissioner Pamela Jones Harbour, *Remarks Before FTC Exploring Privacy Roundtable* (Dec. 7, 2009), *transcript available at* https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf (last visited on Jan. 7, 2026).

Mills + Woods Law, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

E. *University of Phoenix Failed to Comply With Industry Standards.*

54. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

55. The Center for Internet Security's (CIS) Critical Security Controls (CSC) recommends certain best practices to adequately secure data and prevent cybersecurity attacks, including Critical Security Controls of Inventory and Control of Enterprise Assets, Inventory and Control of Software Assets, Data Protection, Secure Configuration of Enterprise Assets and Software, Account Management, Access Control Management, Continuous Vulnerability Management, Audit Log Management, Email and Web Browser Protections, Malware Defenses, Data Recovery, Network Infrastructure Management, Network Monitoring and Defense, Security Awareness and Skills Training, Service Provider Management, Application Software Security, Incident Response Management, and Penetration Testing.[8]

56. The National Institute of Standards and Technology ("NIST") also recommends certain practices to safeguard systems, such as the following:

a. Control who logs on to your network and uses your computers and other devices.
b. Use security software to protect data.
c. Encrypt sensitive data, at rest and in transit.
d. Conduct regular backups of data.
e. Update security software regularly, automating those updates if possible.
f. Have formal policies for safely disposing of electronic files and

[8] *The 18 CIS Critical Security Controls*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/controls/cis-controls-list (last visited on Jan. 7, 2026).

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

old devices.

g. Train everyone who uses your computers, devices, and network about cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

57. Further still, the United States Cybersecurity and Infrastructure Security Agency ("CISA") makes specific recommendations to organizations to guard against cybersecurity attacks, including (a) reducing the likelihood of a damaging cyber intrusion by validating that "remote access to the organization's network and privileged or administrative access requires multi-factor authentication, [e]nsur[ing] that software is up to date, prioritizing updates that address known exploited vulnerabilities identified by CISA[,] [c]onfirm[ing] that the organization's IT personnel have disabled all ports and protocols that are not essential for business purposes," and other steps; (b) taking steps to quickly detect a potential intrusion, including "[e]nsur[ing] that cybersecurity/IT personnel are focused on identifying and quickly assessing any unexpected or unusual network behavior [and] [e]nabl[ing] logging in order to better investigate issues or events[;] [c]onfirm[ing] that the organization's entire network is protected by antivirus/antimalware software and that signatures in these tools are updated," and (c) "[e]nsur[ing] that the organization is prepared to respond if an intrusion occurs," and other steps.[9]

58. Defendant failed to implement industry-standard cybersecurity measures, including by failing to meet the minimum standards of both the NIST Cybersecurity

[9] *Shields Up: Guidance for Organizations*, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, https://www.cisa.gov/shields-guidance-organizations (last visited Jan. 7, 2026).

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

Framework Version 2.0 (including PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established frameworks for reasonable cybersecurity readiness, and by failing to comply with other industry standards for protecting Plaintiffs' and Class Members' Private Information, resulting in the Data Breach.

F. ***University of Phoenix Breached its Duty to Safeguard Plaintiffs' and Class Members' Private Information.***

59. In addition to its obligations under federal and state laws, University of Phoenix 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. University of Phoenix owed a duty to Plaintiffs and Class Members to provide reasonable security, including complying with industry standards and requirements, training for its staff, and ensuring that the systems it used to store students' Private Information adequately protected the Private Information.

60. University of Phoenix breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard the computer systems that housed students' data. University of Phoenix's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

Mills + Woods Law, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect the Private Information in its possession

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

d. Failing to sufficiently train its employees regarding the proper handling of the Private Information in its possession;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

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

g. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

61. University of Phoenix negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access the computer network and systems which contained unsecured and unencrypted Private Information.

62. Had University of Phoenix remedied the deficiencies within the information storage and security systems that housed students' Private Information, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented the theft of Plaintiffs' and Class Members' confidential Private Information.

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

63. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft.

G. *University of Phoenix Should Have Known that Cybercriminals Target Private Information to Carry Out Fraud and Identity Theft.*

64. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data. Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

65. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

66. Because a person's identity is akin to a puzzle, 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 otherwise harass or track the victim. 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 individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

67. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

68. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

69. One such example of this is the development of "Fullz" packages.

70. Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

71. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs'

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

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

72. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[10] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

73. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's

[10] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Jan. 7, 2026).

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

74. PII is data that can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

75. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[11] The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry.

76. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to

[11] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. DEP'T OF JUSTICE (Feb. 10, 2020), https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-four-members-china-s-military (last visited on Jan. 7, 2026).

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

$200, and bank details have a price range of $50 to $200.[12] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web and that the "*fullz*" (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[13]

77. Furthermore, even information such as names, email addresses and phone numbers, can have value to a hacker. Beyond things like spamming customers, or launching phishing attacks using their names and emails, hackers, *inter alia*, can combine this information with other hacked data to build a more complete picture of an individual. It is often this type of piecing together of a puzzle that allows hackers to successfully carry out phishing attacks or social engineering attacks. This is reflected in recent reports, which warn that "[e]mail addresses are extremely valuable to threat actors who use them as part of their threat campaigns to compromise accounts and send phishing emails."[14]

78. The Dark Web Price Index of 2023, published by Privacy Affairs[15] shows how valuable just email addresses alone can be, even when not associated with a financial account:

---

[12] *Your personal data is for sale on the dark web. Here's how much it costs,* DIGITAL TRENDS (Oct. 16, 2019), *available at* https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs (last visited on Jan. 7, 2026).

[13] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web (last visited on Jan. 7, 2026).

[14] *See Dark Web Price Index: The Cost of Email Data,* MAGICSPAM, https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/ (last visited on Jan. 7, 2026).

[15] *See Dark Web Price Index 2023*, PRIVACY AFFAIRS, https://www.privacyaffairs.com/dark-web-price-index-2023/ (last visited on Jan. 7, 2026).

Email Database Dumps	Avg. Price USD (2022)
10,000,000 USA email addresses	$120
600,000 New Zealand email addresses	$110
2,400,000 million Canada email addresses	$100

79. Beyond using email addresses for hacking, the sale of a batch of illegally obtained email addresses can lead to increased spam emails. If an email address is swamped with spam, that address may become cumbersome or impossible to use, making it less valuable to its owner.

80. Likewise, the value of PII is increasingly evident in our digital economy. Many companies including University of Phoenix collect PII for purposes of data analytics and marketing. These companies, collect it to better target customers, and shares it with third parties for similar purposes.[16]

81. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[17]

82. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not only by a price

[16] *See Privacy Policy*, ROBINHOOD, https://robinhood.com/us/en/support/articles/privacy-policy/ (last visited on Jan. 7, 2026).

[17] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets,* 15 Rich. J. L. & Tech. 11, 14 (2009).

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

at which consumers or hackers actually seek to sell it, but rather by the economic benefit consumers derive from being able to use it and control the use of it.

83. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

84. Data breaches, like that at issue here, damage consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiffs' PII impairs their ability to participate in the economic marketplace.

85. The Identity Theft Resource Center documents the multitude of harms caused by fraudulent use of PII in its 2023 Consumer Impact Report.[18] After interviewing over 14,000 identity crime victims, researchers found that as a result of the criminal misuse of their PII:

- 77-percent experienced financial-related problems;
- 29-percent experienced financial losses exceeding $10,000;
- 40-percent were unable to pay bills;
- 28-percent were turned down for credit or loans;
- 37-percent became indebted;
- 87-percent experienced feelings of anxiety;
- 67-percent experienced difficulty sleeping; and

[18] *2023 Consumer Impact Report* (Jan. 2024), IDENTITY THEFT RESOURCE CENTER, *available online at*: https://www.idtheftcenter.org/wp-content/uploads/2023/08/ITRC_2023-Consumer-Impact-Report_Final-1.pdf (last visited on Jan. 7, 2026).

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

- 51-percent suffered from panic of anxiety attacks.[19]

86. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[20]

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

87. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

88. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

///

///

///

---

[19] *Id* at pp 21-25.

[20] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE (June 2007), *available at* https://www.gao.gov/assets/gao-07-737.pdf (last visited on Jan. 7, 2026).

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

H. *Plaintiffs' and Class Members' Damages*

Plaintiff Neblock's Experience

89. Upon information and belief, University of Phoenix's students entrusted Defendant with their Private Information, including the Private Information of Plaintiff Neblock.

90. On or about December 22, 2025, Plaintiff Neblock received the Notice informing her that her Private Information had been involved during the Data Breach. The Notice provided that the Private Information compromised included her "name and Social Security number".

91. The Notice offered Plaintiff Neblock only one year of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff Neblock will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of her Private Information.

92. Plaintiff Neblock suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her accounts for fraud.

93. Plaintiff Neblock would not have provided her Private Information to Defendant had Defendant timely disclosed that it lacked adequate computer and data security practices to safeguard the Private Information in its possession from theft, or that the systems used for storage were subject to a data breach.

94. Plaintiff Neblock suffered actual injury in the form of having her Private Information compromised and/or stolen as a result of the Data Breach.

95. Plaintiff Neblock suffered actual injury in the form of damages to and diminution in the value of her personal information – a form of intangible property that Plaintiff Neblock entrusted to Defendant for the purpose of receiving educational services from Defendant's Client(s) and which was compromised in, and as a result of, the Data Breach.

96. Plaintiff Neblock suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

97. Plaintiff Neblock has a continuing interest in ensuring that her Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches. This interest is particularly acute, as Defendant's systems have already been shown to be susceptible to compromise and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its customers' Private Information.

98. As a result of the Data Breach, Plaintiff Neblock made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant, as well as long-term credit monitoring options she will now need to use. Plaintiff Neblock has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

Mills + Woods Law, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

99. As a result of the Data Breach, Plaintiff Neblock has suffered anxiety as a result of the release of her Private Information to cybercriminals, which Private Information she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of committing cyber and other crimes against her. Plaintiff Neblock is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach will have on her life.

100. Plaintiff Neblock also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of her Private Information, a form of property that Defendant obtained from Plaintiff Neblock; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

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

Plaintiff Wyche's Experience

102. Upon information and belief, University of Phoenix's students entrusted Defendant with their Private Information, including the Private Information of Plaintiff Wyche.

103. On or about December 22, 2025, Plaintiff Wyche received the Notice informing him that his Private Information had been involved during the Data Breach. The

Notice provided that the Private Information compromised included his "name and Social Security number".

104. The Notice offered Plaintiff Wyche only one year of credit monitoring services. One year of credit monitoring is not sufficient given that Plaintiff Wyche will now experience a lifetime of increased risk of identity theft and other forms of targeted fraudulent misuse of his Private Information.

105. Plaintiff Wyche suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring his accounts for fraud.

106. Plaintiff Wyche would not have provided his Private Information to Defendant had Defendant timely disclosed that it lacked adequate computer and data security practices to safeguard the Private Information in its possession from theft, or that the systems used for storage were subject to a data breach.

107. Plaintiff Wyche suffered actual injury in the form of having his Private Information compromised and/or stolen as a result of the Data Breach.

108. Plaintiff Wyche suffered actual injury in the form of damages to and diminution in the value of his personal information – a form of intangible property that Plaintiff Wyche entrusted to Defendant for the purpose of receiving educational services from Defendant's Client(s) and which was compromised in, and as a result of, the Data Breach.

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

109. Plaintiff Wyche suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by his Private Information being placed in the hands of criminals.

110. Plaintiff Wyche has a continuing interest in ensuring that his Private Information, which remains in the possession of Defendant, is protected and safeguarded from future breaches. This interest is particularly acute, as Defendant's systems have already been shown to be susceptible to compromise and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate security and training measures to protect its customers' Private Information.

111. As a result of the Data Breach, Plaintiff Wyche made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendant, as well as long-term credit monitoring options he will now need to use. Plaintiff Wyche has spent several hours dealing with the Data Breach, valuable time he otherwise would have spent on other activities.

112. As a result of the Data Breach, Plaintiff Wyche has suffered anxiety as a result of the release of his Private Information to cybercriminals, which Private Information he believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using his Private Information for purposes of committing cyber and other crimes against him. Plaintiff Wyche is very concerned about this increased, substantial, and continuing risk, as well as

the consequences that identity theft and fraud resulting from the Data Breach will have on his life.

113. Plaintiff Wyche also suffered actual injury as a result of the Data Breach in the form of (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff Wyche; (b) violation of his privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud he now faces.

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

115. In sum, Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

116. Plaintiffs and Class Members entrusted their Private Information to Defendant in order to receive services from Defendant.

117. Plaintiffs' Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which resulted from Defendant's inadequate data security practices.

118. As a direct and proximate result of University of Phoenix's actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns filed in their

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

119. Further, as a direct and proximate result of University of Phoenix's conduct, Plaintiffs and Class Members have been forced to spend time dealing with the effects of the Data Breach.

120. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

121. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

122. Plaintiffs and Class Members also lost the benefit of the bargain they made with University of Phoenix. Plaintiffs and Class Members overpaid for services that were intended to be accompanied by adequate data security but were not. Upon information and belief, Plaintiffs allege that payments made by University of Phoenix's students to University of Phoenix included payment for cybersecurity protection to protect Plaintiffs' and Class Members' Private Information, and that those cybersecurity costs were passed on to Plaintiffs and Class Members in the form of elevated prices charged by University of Phoenix for their services. Thus, Plaintiffs and the Class did not receive what they paid for.

Mills + Woods Law, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

123. Additionally, as a direct and proximate result of University of Phoenix's conduct, Plaintiffs and Class Members have also been forced to 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, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

124. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

125. Additionally, Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[21] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[22]

126. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has

[21] *See How Data Brokers Profit from the Data We Create*, THE QUANTUM RECORD, https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/ (last visited on Jan. 7, 2026).

[22] *Frequently Asked Questions,* NIELSEN COMPUTER & MOBILE PANEL, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited on Jan. 7, 2026).

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

127. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Addressing their inability to withdraw funds linked to compromised accounts;

d. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

e. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

f. Contacting financial institutions and closing or modifying financial accounts;

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

g. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

h. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

i. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

128. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of University of Phoenix, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

129. As a direct and proximate result of University of Phoenix's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

130. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

131. Specifically, Plaintiffs propose the following Nationwide Class (referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
> All individuals in the United States who had Private Information impacted as a result of the Data Breach, including all who were sent a notice of the Data Breach.

132. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

133. Plaintiffs reserve the right to modify or amend the definitions of the proposed Nationwide Class, as well as add subclasses, if necessary, before the Court determines whether certification is appropriate.

134. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

135. **Numerosity.** The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of 348,000 students whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through University of Phoenix's records, publication notice, self-identification, and other means.

Mills + Woods Law, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

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

a. Whether University of Phoenix engaged in the conduct alleged herein;

b. When University of Phoenix learned of the Data Breach;

c. Whether University of Phoenix's response to the Data Breach was adequate;

d. Whether University of Phoenix unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

e. Whether University of Phoenix 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;

f. Whether University of Phoenix's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether University of Phoenix's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether University of Phoenix owed a duty to Class Members to safeguard their Private Information;

i. Whether University of Phoenix breached its duty to Class Members to safeguard their Private Information;

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

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

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

l. Whether University of Phoenix breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

m. Whether University of Phoenix knew or should have known that the data security systems and monitoring processes were deficient;

n. What damages Plaintiffs and Class Members suffered as a result of University of Phoenix's misconduct;

o. Whether University of Phoenix's conduct was negligent;

p. Whether University of Phoenix's conduct was *per se* negligent;

q. Whether University of Phoenix was unjustly enriched;

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.

137. **Typicality**. 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.

138. **Adequacy of Representation.** Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

139. **Predominance.** University of Phoenix has engaged in a common course of conduct toward Plaintiffs and Class Members in that 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 University of Phoenix'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.

140. **Superiority.** A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for University of Phoenix. In contrast,

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

141. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). University of Phoenix has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

142. Finally, all members of the proposed Class are readily ascertainable. University of Phoenix has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by University of Phoenix.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

143. Plaintiffs restate and reallege all of the allegations stated above and hereafter as if fully set forth herein.

144. University of Phoenix knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

145. University of Phoenix knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of

Mills + Woods Law, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

adequate security. University of Phoenix was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

146. University of Phoenix owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to it. University of Phoenix's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect the Private Information in its possession it using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

147. University of Phoenix's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

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.

148. University of Phoenix's duty also arose because Defendant was bound by industry standards to protect the confidential Private Information entrusted to it.

149. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and University of Phoenix owed them a duty of care to not subject them to an unreasonable risk of harm.

150. University of Phoenix, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within University of Phoenix's possession.

151. University of Phoenix, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

152. University of Phoenix, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

153. University of Phoenix breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific

Mills + Woods Law, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

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 the networks and systems that housed Plaintiffs' Private Information;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA;

154. University of Phoenix had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust University of Phoenix with their Private Information was predicated on the understanding that University of Phoenix would take adequate security precautions.

155. University of Phoenix's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised and exfiltrated as alleged herein.

156. As a result of University of Phoenix's ongoing failure to notify Plaintiffs and Class Members regarding exactly what Private Information has been compromised, Plaintiffs and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

157. University of Phoenix's breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

158. As a result of University of Phoenix's negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

159. University of Phoenix also had independent duties under state laws that required it to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach.

160. As a direct and proximate result of University of Phoenix's negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

161. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

162. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

163. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring University of Phoenix to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

///

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

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

164. Plaintiffs restate and reallege the allegations stated above and hereafter as if fully set forth herein.

165. Pursuant to Section 5 of the FTCA, University of Phoenix had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class Members.

166. University of Phoenix breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

167. Plaintiffs and Class Members are within the class of persons that the FTCA is intended to protect.

168. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of University of Phoenix's duty in this regard.

169. University of Phoenix violated the FTCA by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

170. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to University of Phoenix's networks, databases, and computers that stored Plaintiffs' and Class Members' unencrypted Private Information.

171. University of Phoenix's violations of the FTCA constitute negligence *per se*.

172. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to University of Phoenix's negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

173. As a direct and proximate result of University of Phoenix's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

174. University of Phoenix breached its duties to Plaintiffs and the Class under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

175. As a direct and proximate result of University of Phoenix's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

Mills + Woods Law, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

176. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring University of Phoenix to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT III
BREACH OF CONTRACT
(On behalf of Plaintiffs and the Nationwide Class)

177. Plaintiffs restate and reallege all of the allegations stated above and hereafter as if fully set forth herein.

178. Plaintiffs and Class Members entered into a valid and enforceable contract through which they paid money to University of Phoenix in exchange for services. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiffs' and Class Members' Private Information.

179. University of Phoenix's Privacy Policy memorialized the rights and obligations of University of Phoenix and its customers. This document was provided to Plaintiffs and Class Members in a manner in which it became part of the agreement for services.

180. In the Privacy Policy, University of Phoenix commits to protecting the privacy and security of private information and promises to never share Plaintiffs' and Class Members' Private Information except under certain limited circumstances.

181. Plaintiffs and Class Members fully performed their obligations under their contracts with University of Phoenix.

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

182. However, University of Phoenix did not secure, safeguard, and/or keep private Plaintiffs' and Class Members' Private Information, and therefore University of Phoenix breached its contracts with Plaintiffs and Class Members.

183. University of Phoenix allowed third parties to access, copy, and/or exfiltrate Plaintiffs' and Class Members' Private Information without permission. Therefore, University of Phoenix breached the Privacy Policy with Plaintiffs and Class Members.

184. University of Phoenix's failure to satisfy its confidentiality and privacy obligations resulted in University of Phoenix providing services to Plaintiffs and Class Members that were of a diminished value.

185. As a result, Plaintiffs and Class Members have been harmed, damaged, and/or injured as described herein, including in Defendant's failure to fully perform its part of the bargain with Plaintiffs and Class Members.

186. As a direct and proximate result of University of Phoenix's conduct, Plaintiffs and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

187. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring University of Phoenix to, inter alia, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

///

///

///

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

COUNT IV
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Nationwide Class)

188. Plaintiffs restate and reallege all of the allegations stated above and hereafter as if fully set forth herein.

189. This Count is pleaded in the alternative to Count III above.

190. University of Phoenix provides educational services to Plaintiffs and Class Members. Plaintiffs and Class Members formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiffs and Class Members paying for services from Defendant.

191. Through Defendant's sale of services, it knew or should have known that it must protect Plaintiffs' and Class Members' confidential Private Information in accordance with University of Phoenix's policies, practices, and applicable law.

192. As consideration, Plaintiffs and Class Members paid money to University of Phoenix and turned over valuable Private Information to University of Phoenix. Accordingly, Plaintiffs and Class Members bargained with University of Phoenix to securely maintain and store their Private Information.

193. University of Phoenix accepted possession of Plaintiffs' and Class Members' Private Information for the purpose of providing goods and services to Plaintiffs and Class Members.

194. In delivering their Private Information to University of Phoenix and paying for goods and services, Plaintiffs and Class Members intended and understood that

University of Phoenix would adequately safeguard the Private Information as part of that service.

195. Defendant's implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of its employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; and (7) taking other steps to protect against foreseeable data breaches.

196. Plaintiffs and Class Members would not have entrusted their Private Information to University of Phoenix in the absence of such an implied contract.

197. Had University of Phoenix disclosed to Plaintiffs and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and Class Members would not have provided their Private Information to University of Phoenix.

198. University of Phoenix recognized that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiffs and the other Class Members.

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

199. University of Phoenix violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information.

200. Plaintiffs and Class Members have been damaged by University of Phoenix's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT V
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Nationwide Class)

201. Plaintiffs restate and reallege the allegations stated above and hereafter as if fully set forth herein.

202. This Count is pleaded in the alternative to Counts III and IV above.

203. Plaintiffs and Class Members conferred a benefit on University of Phoenix by providing their Private Information to Defendant. Moreover, upon information and belief, Plaintiffs allege that payments made by University of Phoenix's students to University of Phoenix included payment for cybersecurity protection to protect Plaintiffs' and Class Members' Private Information, and that those cybersecurity costs were passed on to Plaintiffs and Class Members in the form of elevated prices charged by University of Phoenix for their educational services. Plaintiffs and Class Members did not receive such protection.

204. Upon information and belief, University of Phoenix funds its data security measures entirely from its general revenue, including payments made to it by its students on behalf of Plaintiffs and Class Members.

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

205. As such, a portion of the payments made by Plaintiffs and Class Members is to be used to provide a reasonable and adequate level of data security that is in compliance with applicable state and federal regulations and industry standards, and the amount of the portion of each payment made that is allocated to data security is known to University of Phoenix.

206. University of Phoenix has retained the benefits of its unlawful conduct, including the amounts of payment indirectly received from Plaintiffs and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

207. University of Phoenix knew that Plaintiffs and Class Members conferred a benefit upon it, which University of Phoenix accepted. University of Phoenix profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes, while failing to use the payments it received for adequate data security measures that would have secured Plaintiffs' and Class Members' Private Information and prevented the Data Breach.

208. If Plaintiffs and Class Members had known that University of Phoenix had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

209. Due to University of Phoenix's conduct alleged herein, it would be unjust and inequitable under the circumstances for University of Phoenix to be permitted to retain the benefit of its wrongful conduct.

210. As a direct and proximate result of University of Phoenix's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

to: (i) the loss of the opportunity to control how their Private Information is used; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (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 identity theft; (v) the continued risk to their Private Information, which remains in University of Phoenix's possession and is subject to further unauthorized disclosures so long as University of Phoenix fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vi) 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.

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

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

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

COUNT VI
DECLARATORY JUDGMENT
(On behalf of Plaintiffs and the Nationwide Class)

213. Plaintiffs restate and reallege the allegations stated above and hereafter as if fully set forth herein.

214. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal statutes described in this Complaint.

215. University of Phoenix owes a duty of care to Plaintiffs and Class Members, which required it to adequately secure Plaintiffs' and Class Members' Private Information.

216. University of Phoenix still possesses Private Information regarding Plaintiffs and Class Members.

217. Plaintiffs allege that University of Phoenix's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

218. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. University of Phoenix owes a legal duty to secure its students' Private Information and to timely notify them of a data breach under the common law and Section 5 of the FTCA;

b. University of Phoenix's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect the Private Information in its possession; and

c. University of Phoenix continues to breach this legal duty by failing to employ reasonable measures to secure its students' Private Information.

219. This Court should also issue corresponding prospective injunctive relief requiring University of Phoenix to employ adequate security protocols consistent with legal and industry standards to protect the Private Information in its possession, including the following:

a. Order University of Phoenix to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, University of Phoenix must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on University of Phoenix's systems on a periodic basis, and ordering University of Phoenix to promptly correct any problems or issues detected by such third-party security auditors;

Mills + Woods Law, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of University of Phoenix's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting 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; and

vii. meaningfully educating its students and their employees about the threats they face with regard to the security of their Private Information, as well as the steps they should take to protect themselves.

220. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at University of Phoenix. The risk of another such breach is real, immediate, and substantial. If another breach at University of Phoenix occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

221. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to University of Phoenix if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of University of Phoenix's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and University of Phoenix has a pre-existing legal obligation to employ such measures.

222. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at University of Phoenix, thus preventing future injury to Plaintiffs, Class Members, and others whose Private Information would be further compromised.

JURY TRIAL DEMAND

223. Plaintiffs demand a trial by jury on all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

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

d. An order instructing University of Phoenix to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring University of Phoenix to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

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

RESPECTFULLY SUBMITTED this 14th day of January 2026.

MILLS + WOODS LAW, PLLC

By */s/ Sean A. Woods*

Robert T. Mills
Sean A. Woods
5055 North 12th Street, Suite 101
Phoenix, AZ 85014

Tyler J. Bean
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151

Attorneys for Plaintiffs and the Putative Class

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

CERTIFICATE OF SERVICE

I hereby certify that on January 14, 2026, I electronically transmitted the foregoing document to the Clerk's Office using the ECF System for filing.

/s/ Ben Dangerfield

MILLS + WOODS LAW, PLLC
5055 North 12th Street, Suite 101
Phoenix, AZ 85014
480.999.4556

UNITED STATES DISTRICT COURT DISTRICT OF ARIZONA

Civil Cover Sheet

This automated JS-44 conforms generally to the manual JS-44 approved by the Judicial Conference of the United States in September 1974. The data is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. The information contained herein neither replaces nor supplements the filing and service of pleadings or other papers as required by law. This form is authorized for use only in the District of Arizona.

The completed cover sheet must be printed directly to PDF and filed as an attachment to the Complaint or Notice of Removal.

Plaintiff(s): **Melissa Neblock , ; Antonyo Wyche , ;**

County of Residence: Outside the State of Arizona

County Where Claim For Relief Arose: Maricopa

Plaintiff's Atty(s):

Sean A. Woods ,
Mills + Woods Law, PLLC
5055 N 12th St., STe. 101
Phoenix, Arizona 85014
(480) 999-4556

Robert T. Mills ,
Mills + Woods Law, PLLC
5055 N 12th St., Ste. 101
Phoenix, Arizona 85202
(480) 999-4556

Defendant(s): **The University of Phoenix, Inc. , ;**

County of Residence: Maricopa

Defendant's Atty(s):

,

,

IFP REQUESTED

REMOVAL FROM COUNTY, CASE #

II. Basis of Jurisdiction: **3. Federal Question (U.S. not a party)**

III. Citizenship of Principal Parties**(Diversity Cases Only)**

6 Foreign State

Plaintiff:-

Defendant:-	**4 AZ corp or Principal place of Bus. in AZ**
IV. Origin :	**1. Original Proceeding**
V. Nature of Suit:	**190 Other Contract**
VI.Cause of Action:	**The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, U.S.C. § 1332(d)(2). Plaintiffs allege violations of 15 U.S.C. § 45, among other claims.**
VII. Requested in Complaint	
Class Action:	**Yes**
Dollar Demand:	
Jury Demand:	**Yes**

VIII. This case **is not related** to another case.

Signature: /s/ Sean A. Woods

Date: 01/14/2026

If any of this information is incorrect, please go back to the Civil Cover Sheet Input form using the *Back* button in your browser and change it. Once correct, save this form as a PDF and include it as an attachment to your case opening documents.

Revised: 01/2014