UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

ELIZABETH TAGUE, on behalf of herself and all others similarly situated, Plaintiff, v. **SAINT LOUIS UNIVERSITY,** Defendant.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Elizabeth Tague, individually and on behalf of herself and all similarly situated persons, alleges the following against Saint Louis University ("SLU" or "Defendant") based upon personal knowledge with respect to herself and on information and belief derived from, among other things, investigation by her counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against SLU for its failure to properly secure and safeguard Plaintiff's and other similarly situated current and former students' and applicants' name and medical information (the "Private Information") from cybercriminals.

2. SLU, based in Saint Louis, University, is a private university that serves thousands of students in their educational pursuits.

3. On or about December 1, 2023, SLU sent out data breach notice letters (the "Notice") to individuals whose information was compromised as a result of the incident.

4. Based on the Notice, SLU discovered that an unauthorized party had access to Plaintiff's and Class Members' (defined below) Private Information between December 2022 and July 2023 (the "Data Breach").

5. Plaintiff and Class Members 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.

6. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, using Class Members' information to obtain medical services.

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

8. Therefore, Plaintiff 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.

9. Plaintiff brings this class action lawsuit to address SLU's inadequate safeguarding of student and applicant Private Information that it collected and maintained.

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

11. Upon information and belief, SLU failed to properly monitor its systems and properly implement adequate data security practices with regard to the computer network and systems that housed the Private Information. Had SLU properly monitored its network, it could have prevented the Data Breach.

12. Plaintiff's and Class Members' identities are now at risk because of SLU's negligent conduct as the Private Information that SLU collected and maintained is now in the hands of data thieves and other unauthorized third parties.

13. Plaintiff seeks to remedy these harms on behalf of herself and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

14. Accordingly, Plaintiff, on behalf of herself and the Class, asserts claims for negligence, negligence *per se*, breach of contract, breach of implied contract, unjust enrichment, and declaratory and injunctive relief.

II. PARTIES

15. Plaintiff Tague is, and at all times mentioned herein was, an individual citizen of the State of Illinois.

16. Defendant Saint Louis University is a private university with campuses located at 1 N. Grand Blvd., St. Louis, Missouri 63103 and Madrid, Spain.

III. JURISDICTION AND VENUE

17. 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 SLU. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

18. This Court has jurisdiction over SLU because SLU operates in and/or is incorporated in this District.

19. 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 SLU has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. SLU's Business and Collection of Plaintiff's and Class Members' Private Information

20. Founded in 1818, SLU "is one of the nation's oldest and most prestigious Catholic Universities … recognized for world-class academics, life-changing research, compassionate health care, and a strong commitment to faith and service."[1]

21. As a condition of receiving a SLU education, SLU requires that its students and faculty members entrust it with highly sensitive personal information. In the ordinary course of receiving service from SLU, Plaintiff and Class Members were required to provide their Private Information to Defendant.

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

23. Plaintiff and Class Members relied on SLU to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this information, which Defendant ultimately failed to do.

[1] *See* https://www.slu.edu/about/index.php (last visited on April 22, 2024).

B. The Data Breach and SLU's Inadequate Notice to Plaintiff and Class Members

24. According to Defendant's Notice, it discovered that an unauthorized party had access to Plaintiff's and Class Members' Private Information between December 2022 and July 2023 (the "Data Breach").

25. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including full names in connection with medical information.

26. SLU had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

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

28. SLU's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

29. SLU knew or should have known that its electronic records would be targeted by cybercriminals.

C. SLU's Failure to Comply with FTC Guidelines Evinces its Negligence

30. 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).

31. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal student 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 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.

32. 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, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

33. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect student 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 the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

34. As evidenced by the Data Breach, SLU failed to properly implement basic data security practices. SLU's failure to employ reasonable and appropriate measures to protect against

unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

35. SLU 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.

D. SLU's Failure to Comply with HIPAA Evinces its Negligence

1. Title II of HIPAA contains what are known as the Administration Simplification provisions. *See* 42 U.S.C. §§ 1301, *et seq*. These provisions require that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI similar to the data Defendant left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

2. SLU's Data Breach resulted from a combination of insufficiencies that indicate SLU failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from SLU's Data Breach that SLU either failed to implement, or inadequately implemented, information security policies or procedures to protect Plaintiffs' and Class Members' PHI.

3. Plaintiffs' and Class Members' Private Information compromised in the Data Breach included "protected health information" as defined by CFR § 160.103.

4. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

5. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

6. Plaintiffs' and Class Members' Private Information included "unsecured protected health information" as defined by 45 CFR § 164.402.

7. Plaintiffs' and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

8. Based upon Defendant's Notice to Plaintiffs and Class Members, SLU reasonably believes that Plaintiffs' and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

9. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

10. SLU reasonably believes that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

11. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

12. Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

13. SLU reasonably believes that Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

14. It is reasonable to infer that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

15. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

16. After receiving notice that they were victims of the Data Breach (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

17. In addition, SLU's Data Breach could have been prevented if SLU had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its students.

18. SLU's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information SLU creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

19. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 also required SLU to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***" (emphasis added).

20. Because SLU has failed to comply with HIPAA, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is also necessary to ensure SLU's approach to information security is adequate and appropriate going forward. SLU still maintains the PHI and other highly sensitive PII of its current and former students, including Plaintiffs and Class Members. Without the supervision of the Court through injunctive relief, Plaintiffs' and Class Members' Private Information remains at risk of subsequent data breaches.

E. SLU Also Failed to Comply with Industry Standards

21. 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.

22. Some industry best practices that should be implemented by businesses like SLU include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

23. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training

staff regarding these points. As evidenced by the Data Breach, Defendant failed to follow these cybersecurity best practices.

24. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

25. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

F. SLU Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information

26. In addition to its obligations under federal and state laws, SLU owed a duty to Plaintiff 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. SLU owed a duty to Plaintiff and Class Members to provide reasonable security, including complying with industry standards and requirements, training for its staff, and ensuring that its computer systems, networks, and protocols adequately protected the Private Information of Class Members.

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

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

b. Failing to adequately protect current and former students' and applicants' Private Information;

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

d. Failing to sufficiently train its employees regarding the proper handling of its student and applicant Private Information;

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 Plaintiff's and Class Members' Private Information.

28. SLU negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

29. Had SLU remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

30. Accordingly, Plaintiff's 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. Plaintiff and Class Members also lost the benefit of the bargain they made with SLU.

G. SLU Should Have Known that Cybercriminals Target Private Information to Carry Out Fraud and Identity Theft

31. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[2] 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.

32. 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.

33. 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

[2] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on May 23, 2023).

information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

34. 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.

35. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's 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 Plaintiff and Class Members.

36. 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.[3] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

37. Identity thieves can also use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or

[3] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited May 23, 2023).

official identification card in the victim's name but with the thief's picture, to obtain medical and/or government benefits, or to file a fraudulent tax return using the victim's information.

38. 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.

39. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[4] 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.

40. 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 $200, and bank details have a price range of $50 to $200.[5] 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.[6]

---

[4] *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, available at https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-fourmembers-china-s-military (last visited on May 23, 2023).

[5] *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 May 23, 2023).

[6] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited on May 23, 2023).

41. Furthermore, even information such as names, email addresses and phone numbers, can have value to a hacker. Beyond things like spamming students, 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."[7]

42. The Dark Web Price Index of 2022, published by PrivacyAffairs[8] shows how valuable just email addresses alone can be, even when not associated with a financial account:

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

43. 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.

44. Likewise, the value of PII is increasingly evident in our digital economy. Many companies, including SLU, collect PII for purposes of data analytics and marketing, likely

[7] *See* https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/ (last visited on May 23, 2023).

[8] *See* https://www.privacyaffairs.com/dark-web-price-index-2022/ (last visited on May 23, 2023).

collecting it to better target students, and then subsequently sharing it with third parties for similar purposes.

45. 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."[9]

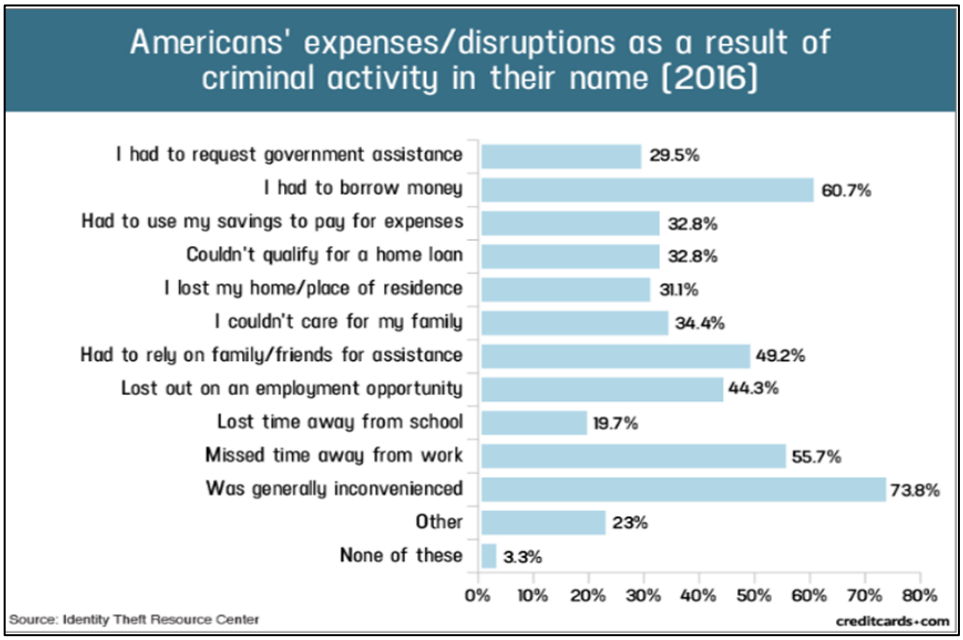
46. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of PII can be derived not only by a price at which consumers or hackers actually seek to sell it, but rather by the economic benefit consumers derive from being able to use it and control the use of it.

47. 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.

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

[9] *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).

49. A study by the Identity Theft Resource Center[10] shows the multitude of harms caused by fraudulent use of PII:



50. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[11]

51. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

52. While credit card information and associated PII can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[12]

---

[10] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited May 23, 2023).

[11] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited on April 22, 2024).

[12] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at*: https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited on April 22, 2024).

53. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

54. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[13]

55. The ramifications of SLU's failure to keep its patients' Private Information secure are long lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

56. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

57. 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 PHI is stolen and when it is

[13] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at*: https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited on April 22, 2024).

misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[14]

> [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.

58. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

59. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft, including medical 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.

H. Plaintiff's and Class Members' Damages

60. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

61. Plaintiff and Class Members entrusted their Private Information to Defendant in order to receive Defendant's educational and related services.

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

63. As a direct and proximate result of SLU's actions and omissions, Plaintiff and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of

[14] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited April 22, 2024).

harm, including but not limited to, having loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

64. Further, as a direct and proximate result of SLU's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach and have incurred costs associated with time spent and the loss of productivity from taking time to address and attempting to ameliorate, mitigate, and deal with the actual and future consequences of the data breach.

65. Plaintiff 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 Plaintiff and Class Members.

66. Additionally, Plaintiff and Class Members have experienced the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach.

67. 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 Plaintiff and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiff and Class Members.

68. Plaintiff and Class Members also lost the benefit of the bargain they made with SLU. Plaintiff and Class Members overpaid for academic services that were intended to be accompanied by adequate data security but were not. Indeed, part of the price Plaintiff and Class Members paid to SLU was intended to be used by SLU to fund adequate security of SLU's system

and protect Plaintiff's and Class Members' Private Information. Thus, Plaintiff and the Class did not receive what they paid for.

69. Plaintiff and Class Members will 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.

70. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information happened with no consideration paid to Plaintiff 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 Plaintiff and Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiff and the Class Members, thereby causing additional loss of value.

71. Finally, Plaintiff 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, monitoring for and discovering fraudulent charges and/or identity theft and the stress, nuisance, and aggravation of dealing with all other issues resulting from the Data Breach.

72. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of SLU, 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.

73. As a direct and proximate result of SLU's actions and inactions, Plaintiff 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

74. Plaintiff brings 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).

75. Specifically, Plaintiff proposes the following Nationwide Class and Illinois Subclass (collectively referred to herein as the "Class"), subject to amendment as appropriate:

> **Nationwide Class**
>
> All individuals in the United States who had Private Information accessed and/or acquired by unauthorized individuals as a result of the Data Breach, including all current and former students and applicants who were sent a notice of the Data Breach.

> **Illinois Subclass**
>
> All individuals in the State of Illinois who had Private Information accessed and/or acquired by unauthorized individuals as a result of the Data Breach, including all current and former students and applicants who were sent a notice of the Data Breach.

76. 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.

77. Plaintiff reserves the right to modify or amend the definition of the proposed Nationwide Class and Illinois Subclass, as well as add subclasses before the Court determines whether certification is appropriate.

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

79. 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 over 93,000 current and former students and applicants whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through SLU's records, Class Members' records, publication notice, self-identification, and other means.

80. 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 SLU engaged in the conduct alleged herein;

b. When SLU learned of the Data Breach;

c. Whether SLU's response to the Data Breach was adequate;

d. Whether SLU unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

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

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

h. Whether SLU owed a duty to Class Members to safeguard their Private Information;

i. Whether SLU breached its duty to Class Members to safeguard their Private Information;

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

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

l. Whether SLU breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

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

n. What damages Plaintiff and Class Members suffered as a result of SLU's misconduct;

o. Whether SLU's conduct was negligent;

p. Whether SLU's conduct was *per se* negligent;

q. Whether SLU was unjustly enriched;

r. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

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

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

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

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

83. Predominance. SLU has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's 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 SLU'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.

84. 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 SLU. In contrast, 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.

85. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). SLU 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.

86. Finally, all members of the proposed Class are readily ascertainable. SLU 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 SLU.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and the Nationwide Class)

87. Plaintiff restates and realleges all of the allegations stated above and hereafter as if fully set forth herein.

88. SLU knowingly collected, came into possession of, and maintained Plaintiff's 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.

89. SLU knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. SLU was on

notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

90. SLU owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. SLU'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 students' Private Information 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 Plaintiff 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 Plaintiff and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

91. SLU'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 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.

92. SLU's duty also arose because Defendant was bound by industry standards to protect its students' confidential Private Information.

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

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

95. SLU, 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 Plaintiff and Class Members.

96. SLU, 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.

97. SLU breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate data security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Allowing unauthorized access to Class Members' Private Information; and

d. Failing to comply with the FTCA.

98. SLU had a special relationship with Plaintiff and Class Members. Plaintiff's and Class Members' willingness to entrust SLU with their Private Information was predicated on the understanding that SLU would take adequate security precautions to protect such Information.

Moreover, only SLU had the ability to protect its systems (and the Private Information that it stored on them) from attack.

99. SLU's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised, exfiltrated, and/or misused, as alleged herein.

100. SLU's breaches of duty also caused a substantial, imminent risk to Plaintiff 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.

101. As a result of SLU's negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff 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.

102. SLU also had independent duties under the FTCA that required it to reasonably safeguard Plaintiff's and Class Members' Private Information.

103. As a direct and proximate result of SLU's negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

104. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

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

106. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring SLU 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 Plaintiff and Class Members.

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

107. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

108. Pursuant to Section 5 of the FTCA, SLU had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and Class Members.

109. SLU 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.

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

111. 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, as well as the industry-standard cybersecurity measures also set forth above, form part of the basis of SLU's duty in this regard.

112. SLU violated the FTCA by failing to use reasonable measures to protect the Private Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

113. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Private Information in compliance with applicable laws would result in an

unauthorized third-party gaining access to SLU's networks, databases, and computers that stored Plaintiff's and Class Members' unencrypted Private Information.

114. SLU's violations of the FTCA constitute negligence *per se*.

115. Plaintiff's and Class Members' Private Information constitutes personal property that was stolen due to SLU's negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

116. As a direct and proximate result of SLU's negligence *per se*, Plaintiff and the Class have suffered, and/or are at a heightened, impending risk of suffering, injuries and damages arising from the unauthorized access and removal of their Private Information from Defendant's systems, including but not limited to damages from the actual misuse of their Private Information and/or the lost time and effort to mitigate the actual and/or potential impact of the Data Breach on their lives.

117. SLU breached its duties to Plaintiff and the Class under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

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

119. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring SLU 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 Plaintiff and Class Members.

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

120. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

121. Plaintiff and Class Members entered into a valid and enforceable contract through which they paid money to SLU in exchange for services. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiff's and Class Members' Private Information.

122. Upon information and belief, SLU's Privacy Policy memorializes the rights and obligations of SLU and its students and was provided to Plaintiff and Class Members upon submission of their student application and/or admission to SLU in a manner in which it became part of the agreement for services.

123. Upon information and belief, SLU's Privacy Policy commits SLU to protecting the privacy and security of private information and promises to never share Plaintiff's and Class Members' Private Information except under certain limited circumstances.

124. Plaintiff and Class Members fully performed their obligations under their contracts with SLU.

125. However, SLU did not secure, safeguard, and/or keep private Plaintiff's and Class Members' Private Information, and therefore SLU breached its contracts with Plaintiff and Class Members.

126. SLU allowed third parties to access, copy, and/or exfiltrate Plaintiff's and Class Members' Private Information without permission. Therefore, SLU breached the Privacy Policy with Plaintiff and Class Members.

127. SLU's failure to satisfy its confidentiality and privacy obligations resulted in SLU providing services to Plaintiff and Class Members that were of a diminished value.

128. As a result, Plaintiff 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 Plaintiff and Class Members.

129. As a direct and proximate result of SLU's conduct, Plaintiff and Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

130. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring SLU 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 Plaintiff and Class Members.

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

131. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

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

133. SLU provides academic services to Plaintiff and Class Members. Plaintiff and Class Members formed an implied contract with Defendant regarding the provision of those services through their collective conduct, including by Plaintiff and Class Members paying for services from Defendant.

134. Through Defendant's sale of academic services, it knew or should have known that it must protect Plaintiff's and Class Members' confidential Private Information in accordance with SLU's policies, practices, and applicable law.

135. As consideration, Plaintiff and Class Members paid money to SLU and turned over valuable Private Information to SLU. Accordingly, Plaintiff and Class Members bargained with SLU to securely maintain and store their Private Information.

136. SLU accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services to Plaintiff and Class Members.

137. In delivering their Private Information to SLU and paying for services, Plaintiff and Class Members intended and understood that SLU would adequately safeguard the Private Information as part of that service.

138. Defendant's implied promises to Plaintiff 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.

139. Plaintiff and Class Members would not have entrusted their Private Information to SLU in the absence of such an implied contract.

140. Had SLU disclosed to Plaintiff and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiff and Class Members would not have provided their Private Information to SLU.

141. SLU recognized that Plaintiff's 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 Plaintiff and the other Class Members.

142. SLU violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class Members' Private Information.

143. Plaintiff and Class Members have been damaged by SLU'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 Plaintiff and the Nationwide Class)

144. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

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

146. Plaintiff and Class Members conferred a benefit on SLU by turning over their Private Information to Defendant and by paying for educational services that should have included cybersecurity protection to protect their Private Information. Plaintiff and Class Members did not receive such protection.

147. Upon information and belief, SLU funds its data security measures entirely from its general revenue, including from payments made to it by Plaintiff and Class Members.

148. As such, a portion of the payments made by Plaintiff 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 SLU.

149. SLU has retained the benefits of its unlawful conduct, including the amounts of payment received from Plaintiff and Class Members that should have been used for adequate cybersecurity practices that it failed to provide.

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

151. If Plaintiff and Class Members had known that SLU had not adequately secured their Private Information, they would not have agreed to provide such Private Information to Defendant.

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

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

appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

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

COUNT VI
ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT
Ill. Comp. Stat. §§505/1, *et seq.*
(On Behalf of Plaintiff Tague and the Illinois Subclass)

156. Plaintiff Tague ("Plaintiff" for purposes of this Count), individually and on behalf of the Illinois Subclass Members, restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

157. The Illinois Consumer Fraud and Deceptive Business Practices Act ("ICFA"), 815 Ill. Comp. Stat. §§505/1, *et seq.*, prohibits unfair methods of competition and unfair or deceptive acts or practices in the conduct of trade or commerce. *See* 815 Ill. Comp. Stat. §505/2. ICFA expressly provides that consideration be given to interpretations by the FTC relating to Section 5 of the FTC Act. *See id*.

158. Plaintiff and the Illinois Subclass Members are a "person," as defined in 815 Ill. Comp. Stat. Ann. §505/1(c), are a "consumer," as defined in 815 Ill. Comp. Stat. Ann. §505/1(e), and satisfy the consumer nexus test in that SLU's unfair and deceptive acts and practices were directed at and impacted the market generally and/or otherwise implicate consumer protection concerns where SLU's unfair and deceptive acts and practices have impacted at least thousands of consumers in Illinois and millions nationwide and remedying SLU's wrongdoing through the relief requested herein would serve the interests of consumers. Furthermore, Plaintiff and the Illinois Subclass Members are consumers located in Illinois, who obtained insurance and health benefits services from SLU.

159. SLU is a "person" as defined by 815 Ill. Comp. Stat. §505/1(c).

160. SLU's conduct as described herein was in the conduct of "trade" or "commerce" as defined by 815 Ill. Comp. Stat. §505/1(f).

161. Under ICFA the use or employment of any practice described in Section 2 of the Uniform Deceptive Trade Practices Act, 815 Ill. Comp. Stat. Ann. §510/2, in the conduct of any trade or commerce is unlawful whether any person has in fact been misled, deceived, or damaged thereby.

162. SLU's deceptive acts and practices include:

a. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Illinois Subclass Members' PII and PHI;

b. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as the Illinois Insurance Information and Privacy Protection Act (215 Ill. Comp. Stat. §5/1014), Illinois Personal Information Protection Act (815 Ill. Comp. Stat. §530/1, *et seq*., Illinois laws regulating the use and disclosure of Social Security Numbers (815 Ill. Comp. Stat. §505/2RR), and the Illinois Uniform Deceptive Trade Practices Act (815 Ill. Comp. Stat. §510/2(a));

c. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and Illinois Subclass Members' PII and PHI, including by failing to reasonably ensure its vendors and business associates reasonably or adequately secured Plaintiff's and Illinois Subclass Members' PII and PHI; and

d. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as the Illinois Insurance Information and Privacy Protection Act (215 Ill. Comp. Stat. §5/1014), Illinois Personal Information Protection Act (815 Ill. Comp. Stat. §530/1, *et seq.*), Illinois laws regulating the use and disclosure of Social Security Numbers (815 Ill. Comp. Stat. §505/2RR), and the Illinois Uniform Deceptive Trade Practices Act (815 Ill. Comp. Stat. §510/2(a)).

163. SLU's unfair acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Illinois Subclass Members' PII and PHI, including by failing to properly secure and encrypt Plaintiff's and Illinois Subclass Members' PII and PHI;

b. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Illinois Subclass Members' PII and PHI, including duties imposed by the FTC Act and HIPAA as well as the Illinois Insurance Information and Privacy Protection Act (215 Ill. Comp. Stat. §5/1014), Illinois Personal Information Protection Act (815 Ill. Comp. Stat. §530/1, *et seq.*), Illinois laws regulating the use and disclosure of Social Security Numbers (815 Ill. Comp. Stat. §505/2RR), and the Illinois Uniform Deceptive Trade Practices Act (815 Ill. Comp. Stat. §510/2(a)); and

c. Failing to comply with the duties imposed by 815 Ill. Comp. Stat. §530/10 and disclose the Data Breach to Plaintiff and the Illinois Subclass Members in a timely and accurate manner.

164. SLU's conduct constitutes unfair methods of competition and unfair practices within the meaning of ICFA because it is immoral, unethical, oppressive, and unscrupulous activity, caused substantial injury to consumers and businesses, and provided no benefit to consumers or competition. SLU cut corners and minimized costs by failing to reasonably ensure Plaintiff's and Illinois Subclass Members' PII and PHI were adequately protected. Further, the

injuries suffered by Plaintiff and the Illinois Subclass Members are not outweighed by any countervailing benefits to consumers or competition. And, because SLU is solely responsible for securing Plaintiff's and Illinois Subclass Members' PII and PHI, there is no way Plaintiff and the Illinois Subclass Members could have known about SLU's inadequate data security practices. By withholding important information from consumers about the inadequacy of its data security, SLU created an asymmetry of information between it and consumers that precluded consumers from taking action to avoid or mitigate injury. There were reasonably available alternatives to further SLU's legitimate business interests.

165. SLU's conduct constitutes unfair practices within the meaning of ICFA because it undermines public policy that businesses protect PII and PHI, as reflected in the FTC Act and HIPAA as well as the Illinois Insurance Information and Privacy Protection Act (215 Ill. Comp. Stat. §5/1014), Illinois Personal Information Protection Act (815 Ill. Comp. Stat. §530/1, *et seq*.), Illinois laws regulating the use and disclosure of Social Security Numbers (815 Ill. Comp. Stat. §505/2RR), and the Illinois Uniform Deceptive Trade Practices Act (815 Ill. Comp. Stat. §510/2(a)).

166. SLU's acts and practices are unfair because SLU's failure to disclose the inadequacies in its data security measures materially interfered with consumers' decision-making in their transactions with SLU. Further, SLU took unreasonable advantage of consumers' lack of understanding about the material risks and costs in their transactions with SLU and consumers' inability to protect themselves due to the asymmetry of information concerning SLU's data security practices.

167. SLU's misrepresentations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of SLU's data security and ability to protect the confidentiality of consumers' PII and PHI.

168. SLU's acts and practices, including its material omissions, were likely to, and did in fact, deceive and mislead members of the public, including students acting reasonably under the circumstances, to their detriment.

169. SLU intended to mislead Plaintiff and Illinois Subclass Members and induce them to rely on its misrepresentations and omissions.

170. SLU had a duty to disclose the above-described facts due to the circumstances of this case and the sensitivity and extent of the PII and PHI in their possession. This duty arose because members of the public, including Plaintiff and the Illinois Subclass Members, bestowed trust and confidence in SLU to keep their PII and PHI secure. SLU's duty to disclose also arose from its possession of exclusive knowledge regarding the security of its vendors' and business associates' systems.

171. Had SLU disclosed to Plaintiff and the Illinois Subclass Members that it did not adequately verify, monitor, and audit the data security measures of its vendors and business associates, SLU would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. SLU was trusted with sensitive and valuable PII and PHI regarding millions of consumers, including Plaintiff and the Illinois Subclass Members. SLU accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and the Illinois Subclass Members acted reasonably in relying on SLU's misrepresentations and omissions, the truth of which they could not have discovered.

172. SLU acted intentionally, knowingly, and maliciously to violate ICFA, and recklessly disregarded Plaintiff's and Illinois Subclass Members' rights.

173. SLU's violations present a continuing risk to Plaintiff and the Illinois Subclass Members as well as to the general public.

174. As a direct and proximate result of SLU's unfair, unlawful, and deceptive trade practices, Plaintiff and the Illinois Subclass Members have suffered and will continue to suffer injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their Private Information, and monetary and non-monetary damages. Specifically, Plaintiff and Illinois Subclass Members have suffered and will continue to suffer a range of injuries, including, but not limited to: (1) a substantially increased and imminent risk of identity theft; (2) the loss of the opportunity to determine how their PII and PHI is used; (3) the compromise, publication, and/or theft of their PII and PHI; (4) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (5) 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; (6) the continued risk to their PII and PHI, which remain in SLU's possession and is subject to further unauthorized disclosures so long as SLU fails to undertake appropriate and adequate measures to protect the PII and PHI in their possession; (7) overpayment for the goods and services that were received without adequate data security; (8) lost value of their PII and PHI; and (9) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of the Data Breach, and thereby suffered ascertainable economic loss.

175. Plaintiff and the Illinois Subclass Members seek all monetary and non-monetary relief allowed by law, including damages, restitution, punitive damages, equitable relief, and reasonable attorney's fees and costs.

COUNT VII
DECLARATORY JUDGMENT
(On behalf of Plaintiff and the Nationwide Class)

176. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

177. 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 FTCA and the industry standards described in this Complaint.

178. SLU owes a duty of care to Plaintiff and Class Members, which required it to adequately secure Plaintiff's and Class Members' Private Information.

179. SLU still possesses Private Information belonging to Plaintiff and Class Members.

180. Plaintiff alleges that SLU's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of her Private Information and the risk remains that further compromises of her Private Information will occur in the future.

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

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

b. SLU'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 students' and applicants' Private Information; and

c. SLU continues to breach this legal duty by failing to employ reasonable measures to secure students' and applicants' Private Information.

182. This Court should also issue corresponding prospective injunctive relief requiring SLU to employ adequate security protocols consistent with legal and industry standards to protect students' and applicants' Private Information, including the following:

a. Order SLU to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, SLU 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 SLU's systems on a periodic basis, and ordering SLU to promptly correct any problems or issues detected by such third-party security auditors;

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 SLU'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 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.

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

184. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to SLU if an injunction is issued. Plaintiff 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 SLU's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and SLU has a pre-existing legal obligation to employ such measures.

185. 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 SLU, thus preventing future injury to Plaintiff and other students whose Private Information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and the Class described above, seeks 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 Plaintiff is a proper representative of the Nationwide Class and Illinois Subclass requested herein;

b. Judgment in favor of Plaintiff 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 SLU to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

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

f. A judgment in favor of Plaintiff 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.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: April 22, 2024

Respectfully submitted,

/s/ Michael D. Pospisil
Michael D. Pospisil #49139MO
Matthew T. Swift #63601
POSPISIL SWIFT, LLC
1600 Genessee Street, Ste. 340
Kansas City, MO. 64102
Tel: (816) 895*6440
Fax: (816) 895-9161
mdp@pslawkc.com
mts@pslawkc.com

Mason A. Barney*
Tyler J. Bean*
SIRI & GLIMSTAD LLP
745 Fifth Avenue, Suite 500
New York, New York 10151
Tel: (212) 532-1091
mbarney@sirillp.com
tbean@sirillp.com

**pro hac vice applications forthcoming*

Attorneys for Plaintiff and the Putative Class