IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

SARA AMES, individually and on behalf of all others similarly situated, Plaintiff, v. SAINT XAVIER UNIVERSITY, Defendant.	Case No.: 1:24-cv-12027 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Sara Ames ("Plaintiff"), individually and on behalf of all others similarly situated, brings this class action against Defendant Saint Xavier University ("Defendant" or "SXU"), and alleges as follows:

JURISDICTION AND VENUE

1. This Court has subject-matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) because (1) the matter in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, (2) the action is a class action, (3) there are members of the proposed Class who are diverse from Defendant, and (4) there are more than 100 proposed Class members.

2. This Court has general personal jurisdiction over Defendant because Defendant is a resident and citizen of this district, Defendant conducts substantial business in this district, and the events giving rise to Plaintiff's claims arise out of Defendant's contacts with this district.

3. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) because Defendant is a resident and citizen of this district.

PARTIES

4. Plaintiff Sara Ames is a resident and citizen of Illinois.

5. Defendant Saint Xavier University is a not-for-profit corporation organized under the laws of Illinois, with its principal place of business located at 3700 W 103rd St., Chicago, Illinois, 60655.

FACTUAL ALLEGATIONS

Saint Xavier University

6. Defendant SXU is a four-year private university. SXU represents, on its website, that it "educates persons to search for truth, to think critically, to communicate effectively and to serve wisely and compassionately in support of human dignity and the common good."[1]

7. In the ordinary course of applying for admission to SXU, each applicant must provide (and Plaintiff did provide) Defendant with Personally Identifiable Information ("PII") including his or her Social Security number, financial information and contact information.

8. Defendant SXU's Privacy Policy touts that "Saint Xavier University takes extensive precautions to protect your personal information both online and offline. Whenever Saint Xavier University collects sensitive personal or financial information via its website, that information is encrypted and transmitted to us in a secure way."[2]

9. As a Business Entity, with an acute interest in maintaining the confidentiality of the PII entrusted to it, Defendant is well-aware of the numerous data breaches that have occurred throughout the United States and its responsibility for safeguarding PII in its possession.

[1] *See* https://www.sxu.edu/about/index.html (last accessed Nov. 20, 2024).
[2] *See* https://www.sxu.edu/about/privacy.html (last accessed Nov. 20, 2024)

The Data Breach

10. According to Defendant, "In July 2023, Saint Xavier University became aware of potential suspicious activity within our computer systems." ("the Data Breach").[3]

11. Defendant claims that "Accordingly, SXU quickly took steps to contain the activity, confirm the security of our systems, and begin a comprehensive investigation to determine the full nature, scope and impact of the activity. The investigation determined that an unauthorized actor downloaded certain files stored on limited SXU systems between June 29, 2023, and July 18, 2023."[4]

12. Defendant further represented that the information compromised included "Social Security numbers, driver's license or state identification card numbers, passport information, financial account information, medical information, biometric information, health insurance information, student identification numbers, dates of birth, payment card information, and account access information" may have been compromised by the Data Breach".[5]

13. According to a notice of data breach filed with the Attorney General of Maine, the Data Breach has affected 212,267 individuals.[6]

14. Defendant began notifying affected individuals by sending them personally addressed Notice Letters on or about October 30, 2024.[7]

[3] *See* https://www.sxu.edu/sxu-notice-of-data-security-incident.pdf (last accessed Nov. 20, 2024).
[4] *Id.*
[5] *Id.*
[6] *See* Data Breach Notifications, Office of the Maine Attorney General, https://www.maine.gov/cgi-bin/agviewerad/ret?loc=1469 (last accessed Nov. 20, 2024).
[7] *See* Notice of Data Security Incident addressed to Plaintiff, attached hereto as Exhibit 1 ("Notice Letter").

15. The Notice Letter addressed to Plaintiff informed her Defendant's investigation determined that specifically her "name, Social Security number, and financial account information" were compromised in the Data Breach.[8]

16. Defendant did not inform affected individuals of the root cause of the Data Breach.[9]

17. Defendant did not state why it waited over 15 months to inform affected individuals after its discovery of the Data Breach.

18. Defendant failed to prevent the data breach because it did not adhere to commonly accepted security standards and failed to detect that its databases were subject to a security breach.

Injuries to Plaintiff and the Class

19. On or about October 30, 2024, Plaintiff received a breach notification letter from Defendant indicating that her PII was compromised during the Data Breach.[10]

20. As a result of the Data Breach, Plaintiff has suffered severe emotional distress and anxiety knowing that her name and Social Security number may have been impacted.

21. Plaintiff is very concerned about the theft of her PII and anticipates spending substantial amounts of time and energy aimed at thwarting adverse effects as a result of the Data Breach.

22. As a direct and proximate result of Defendant's actions and omissions in failing to protect Plaintiff's PII, Plaintiff and the Class have been damaged.

23. Plaintiff and the Class have been placed at a substantial risk of harm in the form of credit fraud or identity theft and have incurred and will likely incur additional damages, including

[8] *Id.*
[9] *Id.*
[10] *Id.*

spending substantial amounts of time monitoring accounts and records, in order to prevent and mitigate credit fraud, identity theft, and financial fraud.

24. In addition to the irreparable damage that may result from the theft of PII, identity theft victims must spend numerous hours and their own money repairing the impacts caused by this breach. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[11]

25. Plaintiff and the Class will spend substantial time and expense (a) monitoring their accounts to identify fraudulent or suspicious charges; (b) cancelling and reissuing cards; (c) purchasing credit monitoring and identity theft prevention services; (d) attempting to withdraw funds linked to compromised, frozen accounts; (e) removing withdrawal and purchase limits on compromised accounts; (f) communicating with financial institutions to dispute fraudulent charges; (g) resetting automatic billing instructions and changing passwords; (h) freezing and unfreezing credit bureau account information; (i) cancelling and re-setting automatic payments as necessary; (j) paying late fees and declined payment penalties as a result of failed automatic payments; and (k) managing the severe anxiety that has been caused by their being personally threatened.

26. Plaintiff and the Class have suffered severe emotional distress as a result of their PII being compromised and will continue to suffer for an indefinite period of time. Since Plaintiff and the Class may not change their Social Security numbers, their heightened risk of becoming victims of fraud is now permanent. Plaintiff and the Class will remain aware of both this permanent risk as well as their permanent inability to cure that risk until it manifests itself in the form of fraud.

[11] U.S. Dep't of Justice, *Victims of Identity Theft*, *2014* (Nov. 13, 2017), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

27. Additionally, Plaintiff and the Class have suffered or are at increased risk of suffering from, *inter alia*, the loss of the opportunity to control how their PII is used, the diminution in the value and/or use of their PII entrusted to Defendant, and loss of privacy.

The Value of PII

28. It is well known that PII, and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

29. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.[12]

30. People place a high value not only on their PII, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.[13]

31. People are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers."[14] There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiff and Class members cannot obtain new numbers unless they become a victim of social security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a

[12] Javelin Strategy & Research, *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study* (Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin.

[13] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf.

[14] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html.

fresh start."[15] The Social Security Administration's reactive security measures make Plaintiff and Class Members especially prone to severe anxiety and emotional distress. Victims of a data breach must remain conscious of their vulnerability to identity theft, awaiting nefarious use of their social security information, while knowing they may not receive protection from that misuse until after it has occurred.

32. Defendant acknowledged the immense value that PII has to Plaintiff and the Class insofar as they sent them a document outlining "What You Can Do" and provided that individuals remain vigilant by "reviewing and monitoring their accounts over the next 12 to 24 months.". However, the document that guides Plaintiff and the Class in protecting their PII serves to emphasize that Defendant has placed the onus on those affected to retain the value of their PII.

Industry Standards for Data Security

33. In light of the numerous high-profile data breaches targeting businesses like Target, Neiman Marcus, eBay, Anthem, Deloitte, Equifax, and Capital One. Defendant is, or reasonably should have been, aware of the importance of safeguarding PII, as well as of the foreseeable consequences of its systems being breached.

34. Security standards commonly accepted among Businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

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

e. Monitoring for suspicious or unknown users;

[15] Social Security Admin., *Identity Theft and Your Social Security Number*, at 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf.

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for PII;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

35. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[16] and protection of PII[17] which includes basic security standards applicable to all types of businesses.

36. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings

[16] Start with Security: A Guide for Business, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[17] Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting personalinformation.pdf.

that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

37. The FTC has also issued guidance on reactive measures entities should take after they have suffered a data breach. Notably, the FTC advises that such entities should not "make misleading statements about the breach" or "withhold key details that might help consumers protect themselves and their information."[18]

38. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, 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 Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[19]

39. Because Defendant was entrusted with consumers' PII, it had, and has, a duty to its consumers to keep their PII secure.

[18] Federal Trade Commission, *Data Breach Response: A Guide for Business,* https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business.
[19] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement.

40. Consumers, such as Plaintiff and the Class, reasonably expect that when they provide PII to entities, such as Defendant, or when those entities forward their PII to other companies, that their PII will be safeguarded.

41. Nonetheless, Defendant failed to prevent the Data Breach. Had Defendant properly maintained and adequately protected its systems, it could have prevented the Data Breach.

CLASS ACTION ALLEGATIONS

42. Plaintiff, individually and on behalf of all others, brings this class action pursuant to Fed. R. Civ. P. 23.

43. The proposed Class are defined as follows:

> All persons whose PII was maintained on Defendant's servers and was compromised in the Data Breach.

44. Plaintiff reserves the right to modify, change, or expand the definitions of the proposed Class based upon discovery and further investigation.

45. *Numerosity*: The proposed Class is so numerous that joinder of all members is impracticable. Although the precise number is not yet known to Plaintiff, Defendant has reported that the number of persons affected by the Data Breach is 212,267 people.[20] The Class members can be readily identified through Defendant's records.

46. *Commonality*: Questions of law or fact common to the Class include, without limitation:

a. Whether Defendant owed a duty or duties to Plaintiff and the Class to exercise due care in collecting, storing, safeguarding, and obtaining their PII;

b. Whether Defendant breached that duty or those duties;

[20] *See supra* fn 6.

c. Whether Defendant failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records to protect against known and anticipated threats to security;

d. Whether the security provided by Defendant was satisfactory to protect customer information as compared to industry standards;

e. Whether Defendant misrepresented or failed to provide adequate information to customers regarding the type of security practices used;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiff's and the Class's PII secure and prevent loss or misuse of that PII;

g. Whether Defendant acted negligently in connection with the monitoring and protecting of Plaintiff's and Class's PII;

h. Whether Defendant's conduct was intentional, willful, or negligent;

i. Whether Defendant violated any and all statutes and/or common law listed herein;

j. Whether the Class suffered damages as a result of Defendant's conduct, omissions, or misrepresentations; and

k. Whether the Class is entitled to injunctive, declarative, and monetary relief as a result of Defendant's conduct.

47. *Typicality*: The claims or defenses of Plaintiff are typical of the claims or defenses of the Class. Class members were injured and suffered damages in substantially the same manner as Plaintiff, Class members have the same claims against Defendant relating to the same course of conduct, and Class members are entitled to relief under the same legal theories asserted by Plaintiff.

48. *Adequacy*: Plaintiff will fairly and adequately protect the interests of the proposed Class and has no interests antagonistic to those of the proposed Class. Plaintiff has retained counsel experienced in the prosecution of complex class actions including, but not limited to, data breaches.

49. *Predominance*: Questions of law or fact common to proposed Class members predominate over any questions affecting only individual members. Common questions such as whether Defendant owed a duty to Plaintiff and the Class and whether Defendant breached its duties predominate over individual questions such as measurement of economic damages.

50. *Superiority*: A class action is superior to other available methods for the fair and efficient adjudication of these claims because individual joinder of the claims of the Class is impracticable. Many members of the Class are without the financial resources necessary to pursue this matter. Even if some members of the Class could afford to litigate their claims separately, such a result would be unduly burdensome to the courts in which the individualized cases would proceed. Individual litigation increases the time and expense of resolving a common dispute concerning Defendant's actions toward an entire group of individuals. Class action procedures allow for far fewer management difficulties in matters of this type and provide the unique benefits of unitary adjudication, economies of scale, and comprehensive supervision over the entire controversy by a single judge in a single court.

51. *Manageability*: Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

52. The Class may be certified pursuant to Rule 23(b)(2) because Defendant has acted on grounds generally applicable to the Class, thereby making appropriate final injunctive relief or corresponding declaratory relief with respect to the Class as a whole.

53. The Class may also be certified pursuant to Rule 23(b)(3) because questions of law and fact common to the Class will predominate over questions affecting individual members, and a class action is superior to other methods for fairly and efficiently adjudicating the controversy and causes of action described in this Complaint.

54. Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

CAUSES OF ACTION

COUNT I
NEGLIGENCE/ NEGLIGENCE PER SE

55. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

56. Defendant owed a duty of care to Plaintiff and Class members to use reasonable means to secure and safeguard the entrusted PII, to prevent its unauthorized access and disclosure to third parties, to guard it from theft, and to detect any attempted or actual breach of its systems. These common law duties existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and Class members would be harmed by the failure to protect their PII because hackers routinely attempt to steal such information and use it for nefarious purposes, but Defendant knew that it was more likely than not Plaintiff and Class members would be harmed by such exposure of their PII.

57. Defendant's duties to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC 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 PII. Various FTC publications and data security breach orders further form the basis of Defendant's duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

58. Defendant's violations of Section 5 of the FTC Act constitute negligence per se.

59. Defendant breached the aforementioned duties when it failed to use security practices that would protect the PII provided to it by Plaintiff and Class members, thus resulting in unauthorized third-party access to the Plaintiff's and Class members' PII.

60. Defendant further breached the duties by failing to design, adopt, implement, control, manage, monitor, update, and audit its processes, controls, policies, procedures, and protocols to comply with the applicable laws reasonable standards of care necessary to safeguard and protect Plaintiff's and Class members' PII within its possession, custody, and control.

61. As a direct and proximate cause of failing to use appropriate security practices, Plaintiff's and Class members' PII was disseminated and made available to unauthorized third parties.

62. Defendant admitted that Plaintiff's and Class members' PII was wrongfully disclosed as a result of the breach.

63. The breach caused direct and substantial damages to Plaintiff and Class members, as well as the possibility of future and imminent harm through the dissemination of their PII and the greatly enhanced risk of credit fraud or identity theft.

64. By engaging in the forgoing acts and omissions, Defendant committed the common law tort of negligence. For all the reasons stated above, Defendant's conduct was negligent and departed from reasonable standards of care including by, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; and failing to provide adequate and appropriate supervision of persons having access to Plaintiff's and Class members' PII.

65. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and the Class, their PII would not have been compromised.

66. Neither Plaintiff nor the Class contributed to the breach or subsequent misuse of their PII as described in this Complaint. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and the Class have been put at an increased risk of credit fraud or identity theft, and Defendant has an obligation to mitigate damages by providing adequate credit and identity monitoring services. Defendant is liable to Plaintiff and the Class for the reasonable costs of future credit and identity monitoring services for a reasonable period of time, substantially in excess of one year. Defendant is also liable to Plaintiff and the Class to the extent that they have directly sustained damages as a result of identity theft or other unauthorized use of their PII, including the amount of time Plaintiff and the Class have spent and will continue to spend as a result of Defendant's negligence. Defendant is also liable to Plaintiff and the Class to the extent their PII has been diminished in value because Plaintiff and the Class no longer control their PII and to whom it is disseminated. Defendant is further liable to Plaintiff and the Class to the extent that they have suffered anxiety and emotional distress as a result of their heightened risk of becoming victims of credit fraud and identity theft.

COUNT II
INVASION OF PRIVACY

67. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

68. Plaintiff and Class members have objective reasonable expectations of solitude and seclusion in their personal and private information and the confidentiality of the content of personal information and non-public medical information.

69. Defendant invaded Plaintiff's and the Class's right to privacy by allowing unauthorized access to their PII and by negligently maintaining the confidentiality of Plaintiff's and the Class's PII, as set forth above.

70. The intrusion was offensive and objectionable to Plaintiff, the Class, and to a reasonable person of ordinary sensibilities in that Plaintiff's and the Class's PII was disclosed without prior written authorization from Plaintiff and the Class.

71. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiff and the Class provided and disclosed their PII to Defendant privately with an intention that the PII would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable to believe that such information would be kept private and would not be disclosed without their written authorization.

72. As a direct and proximate result of Defendant's above acts, Plaintiff's and the Class's PII was viewed, distributed, and used by persons without prior written authorization and Plaintiff and the Class suffered damages as described herein.

73. Defendant is guilty of oppression, fraud, or malice by permitting the unauthorized disclosure of Plaintiff's and the Class's PII with a willful and conscious disregard of their right to privacy.

74. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause Plaintiff and the Class severe and irreparable injury in that the PII maintained by Defendant can be viewed, printed, distributed, and used by unauthorized persons. Plaintiff and the Class have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiff and the Class, and Defendant may freely treat Plaintiff's and the Class's PII with sub-standard and insufficient protections.

COUNT III
UNJUST ENRICHMENT

75. Plaintiff hereby incorporates by reference all preceding paragraphs as though fully set forth herein.

76. Plaintiff and the Class have an interest, both equitable and legal, in their PII that was conferred upon, collected by, and maintained by Defendant and that was ultimately compromised in the data breach.

77. Defendant, by way of its acts and omissions, knowingly and deliberately enriched itself by saving the costs it reasonably should have expended on cybersecurity measures to secure Plaintiff's and the Class's PII.

78. Defendant also understood and appreciated that the PII pertaining to Plaintiff and the Class was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

79. Instead of providing for a reasonable level of security that would have prevented the breach—as is common practice among businesses entrusted with such PII—Defendant instead made a conscious and opportunistic calculation to increase its own profits at the expense of Plaintiff's and the Class's security. Nevertheless, Defendant continued to obtain the benefits conferred on it by Plaintiff and the Class. The benefits conferred upon, received, and enjoyed by Defendant were not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendant to retain these benefits.

80. Plaintiff and the Class suffered as a direct and proximate result of Defendant's decision to profit rather than provide requisite security, and the resulting breach disclosing Plaintiff's and the Class's PII, Plaintiff and the Class suffered and continue to suffer considerable injuries in the forms of, *inter alia,* attempted identity theft, time and expenses mitigating harms,

diminished value of PII, loss of privacy, increased risk of harm, and severe anxiety and emotional distress.

81. Thus, Defendant engaged in opportunistic conduct in spite of its duties to Plaintiff and the Class, wherein it profited from interference with the Plaintiff's and the Class's legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its conduct.

82. Accordingly, Plaintiff, on behalf of herself and the Class, respectfully request that this Court award relief in the form of restitution or disgorgement in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including specifically, the amounts that Defendant should have spent to provide reasonable and adequate data security to protect Plaintiff's and the Class's PII, and/or compensatory damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, prays for a judgment against Defendant as follows:

a. For an order certifying the proposed Class, appointing Plaintiff as Representative of the proposed Class, and appointing the law firms representing Plaintiff as counsel for the Class;

b. For compensatory and punitive and treble damages in an amount to be determined at trial;

c. Payment of costs and expenses of suit herein incurred;

d. Both pre-and post-judgment interest on any amounts awarded;

e. Payment of reasonable attorneys' fees and expert fees;

f. Such other and further relief as the Court may deem proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands trial by jury.

Dated: November 21, 2024

Respectfully submitted,

By: /s/ *Gary M. Klinger*

Gary M. Klinger (IL Bar No. 6303726)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Charles E. Schaffer*
LEVIN SEDRAN & BERMAN LLP
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Tel: (215) 592-1500
cschaffer@lfsblaw.com

Jeffrey S. Goldenberg*
GOLDENBERG SCHNEIDER, LPA
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
Tel: (513) 345-8291
jgoldenberg@gs-legal.com

Brett R. Cohen*
LEEDS BROWN LAW, P.C.
One Old Country Road, Suite 347
Carle Place, NY 11514
Tel: (516) 873-9550
bcohen@leedsbrownlaw.com

Counsel for Plaintiff and Proposed Class

**Pro Hac Vice Forthcoming*