UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA

ELIZABETH GOLEC, individually and on behalf of all others similarly situated, Plaintiff, v. EDUCATIONAL COMPUTER SYSTEMS, INC. d/b/a HEARTLAND ECSI, Defendant.	Case No. 2:24-cv-00699 **COMPLAINT-CLASS ACTION** JURY DEMAND

Plaintiff Elizabeth Golec ("Plaintiff") brings this class action against Defendant Educational Computer Systems, Inc. d/b/a Heartland ECSI ("ECSI" or "Defendant") for its failure to properly secure and safeguard Plaintiff's and Class Members' personally identifiable information ("PII") and financial information stored within Defendant's information network.

INTRODUCTION

1. Defendant ECSI provides schools and colleges with services related to past-due accounts receivable management, campus-based student loan servicing, tax document services, tuition payment plans, refund management, call center, and outsourcing services. ECSI is a subsidiary of Global Payments Inc. Educational Computer Systems.[1]

2. As part of its business, ECSI acquired, collected, and stored Plaintiff's and Class Members' PII and financial information, largely related to loans or financial accounts that Plaintiff and Class Members had with colleges or universities.

3. PII generally incorporates information that can be used to distinguish or trace an

[1] *See* https://www.jdsupra.com/legalnews/educational-computer-systems-announces-4542037/ (last accessed May 9, 2024).

individual's identity, and is generally defined to include certain identifiers that do not on their face name an individual, but that is considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

4. Despite handling highly confidential PII and financial information, ECSI failed to institute proper security protocols to protect this information.

5. Specifically, ECSI had an online form where individuals could search and access tax and financial records without having to login or verify their identity.[2]

6. Third-party cybercriminals, after discovering this security flaw, used this search function to extract Plaintiff's and Class Members' PII and financial information, including tax forms with their Social Security numbers and information about their tuition, scholarships, and student loan payments, from October 29, 2023 until February 12, 2024 (the "Data Breach").[3]

7. As a result of ECSI's failure to adequately protect Plaintiff's and Class Members' PII and financial information, tens or hundreds of thousands of individuals had their data exposed, and now face substantial risks of financial fraud and identity theft, among other risks.

8. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII and financial information was safeguarded, failing to take available steps to prevent unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use.

9. Plaintiff and Class Members are entitled to actual and punitive damages as a result

[2] *Id.*
[3] *Id.*

of Defendant's failure to safeguard their data, and are also entitled to injunctive and other equitable relief to ensure that their information is now and remains secure.

JURISDICTION AND VENUE

10. Jurisdiction is proper in this Court under 28 U.S.C. §1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one class member is a citizen of a state different from Defendant.

11. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. §1367.

12. Defendant is headquartered and routinely conducts business in the Commonwealth where this district is located, has sufficient minimum contacts in this Commonwealth, and has intentionally availed itself of this jurisdiction by marketing and selling products and services, and by accepting and processing payments for those products and services within this Commonwealth.

13. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Plaintiff's claims occurred within this District, and Defendant does business in this Judicial District.

THE PARTIES

Plaintiff Elizabeth Golec

14. Plaintiff Elizabeth Golec is an adult individual and, at all relevant times herein, a resident and citizen of Rhode Island, residing in Coventry, Rhode Island. Plaintiff is a victim of the Data Breach.

15. As required in order to obtain services from Defendant, Plaintiff provided her

highly confidential personal financial information to Defendant, who then possessed, stored, and controlled it.

16. As a result, Plaintiff's information was among the data accessed by an unauthorized third-party in the Data Breach.

17. At all times herein relevant, Plaintiff is and was a member of the Class.

18. Plaintiff received a letter from Defendant, dated April 9, 2024, stating that her PII and financial information was involved in the Data Breach (the "Notice").

19. Plaintiff was unaware of the Data Breach until receiving the Notice.

20. Since receiving the Notice, Plaintiff has been injured in the form of lost time dealing with the consequences of the breach, including: time spent verifying the legitimacy and impact of the Data Breach; time spent exploring credit monitoring and identity theft insurance options; time spent self-monitoring her accounts with heightened scrutiny and time spent seeking legal counsel regarding her options for remedying and/or mitigating the effects of the Data Breach.

21. Plaintiff was also injured by the material risk to future harm she suffers based on Defendant's breach. This risk is imminent and substantial because Plaintiff's data that was exposed in the breach, including financial information and Social Security information, is highly sensitive and presents a high risk of identity theft or fraud; and it is likely, given Defendant's clientele, that some of the Class's information that has been exposed has already been misused.

22. Plaintiff suffered actual injury in the form of damages to and diminution in the value of her PII—a condition of intangible property that they entrusted to Defendant, which was compromised in and as a result of the Data Breach.

23. Plaintiff, as a result of the Data Breach, has dealt with increased anxiety due to her loss of privacy and over the impact of cybercriminals accessing, using, and selling her PII and

financial information.

24. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and financial information, in combination with her name, being placed in the hands of unauthorized third parties/criminals.

25. Plaintiff has a continuing interest in ensuring that her PII and financial information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Defendant Educational Computer Systems, Inc. d/b/a Heartland ECSI

26. Defendant Educational Computer Systems, Inc. d/b/a Heartland ECSI is a Pennsylvania corporation headquartered at 1200 Cherrington Parkway, Suite 200, Coraopolis, Pennsylvania 15108.

COMMON FACTUAL ALLEGATIONS

The Data Breach

27. Defendant ECSI provides schools and colleges with services related to past-due accounts receivable management, campus-based student loan servicing, tax document services, tuition payment plans, refund management, call center, and outsourcing services. ECSI is a subsidiary of Global Payments Inc. Educational Computer Systems.

28. Defendant acquired, collected, and stored Plaintiff's and Class Members' PII and financial information, including information about tuition, scholarships, and loans related to individuals' relationships with colleges and universities.

29. Defendant knew or should have known that Plaintiff and Class Members store and/or share sensitive data, including highly confidential PII and financial information, using Defendant's loan servicing and accounts receivable services, among Defendant's other operations.

30. Despite maintaining such sensitive personal and financial information, Defendant created a significant security risk to this data when it created a "guest tax search functionality" on its website, which allowed anyone on the internet to access tax forms online without logging into a user profile and confirming the user's identity.

31. After discovering this security flaw, on October 29, 2023, unauthorized third-party cybercriminals began using and manipulating the "guest tax search functionality" to access to Plaintiff's and Class Members' PII and financial information as hosted with ECSI, including confidential tax documents such as 1098-E and 1098-T forms. These cybercriminals continued to access Plaintiff's and Class Members' PII and financial information until approximately February 12, 2024.

32. These cybercriminals stole Plaintiff's and Class Members' information with the intent of engaging in the misuse of the PII and financial information by engaging in financial fraud and marketing and selling Plaintiff's and Class Members' PII and financial information.

33. The total number of individuals who have had their data exposed due to Defendant's failure to implement appropriate security safeguards is unknown at this time but is estimated to be in the tens or hundreds of thousands based on Defendant's role in the loan servicing business.

Defendant's Failed Response to the Breach

34. ECSI did not become aware of the breach until February 12, 2024, after the breach had been ongoing for several months. Upon discovering the breach, ECSI eliminated the guest tax search functionality.

35. Two months later, on April 19, 2024, ECSI filed the Notice with the Attorney General of Maine that information belonging to students and other individuals affiliated with an

array of colleges and universities was compromised as a result of significant data security flaws in its network and online search functions.

36. Thus, not until months after it claims to have discovered the Data Breach did ECSI begin sending the Notice to persons whose PII and financial information Defendant believed was potentially compromised as a result of the Data Breach.

37. The Notice included, *inter alia*, basic details of the Data Breach, Defendant's recommended next steps, and Defendant's claims that it had learned of the Data Breach on February 12, 2024, and completed a review thereafter.

38. Upon information and belief, the unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PII and financial information with the intent of engaging in the misuse of the PII and financial information, including marketing and selling Plaintiff's and Class Members' PII.

39. Defendant had and continues to have obligations, applicable federal and state law as set forth herein, reasonable industry standards, common law, and its own assurances and representations to keep Plaintiff's and Class Members' PII confidential and to protect such PII from unauthorized access.

40. Plaintiff and Class Members were required to provide their PII and financial information to Defendant as a result of their dealings, and in furtherance of this relationship, Defendant created, collected, and stored Plaintiff's and Class Members' PII and financial information with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

41. Despite this, Plaintiff and the Class Members remain, even today, in the dark

regarding what particular data was stolen, the particular malware used, and what steps are being taken, if any, to secure their PII and financial information going forward.

42. Plaintiff and Class Members are, thus, left to speculate as to where their PII ended up, who has used it, and for what potentially nefarious purposes, and are left to further speculate as to the full impact of the Data Breach and how exactly Defendant intends to enhance its information security systems and monitoring capabilities to prevent further breaches.

43. Unauthorized individuals can now easily access the PII and/or financial information of Plaintiff and Class Members.

Defendant Collected/Stored Class Members' PII and financial information

44. Defendant acquired, collected, and stored and assured reasonable security over Plaintiff's and Class Members' PII and financial information.

45. As a condition of its relationships with Plaintiff and Class Members, Defendant required that Plaintiff and Class Members entrust Defendant with highly sensitive and confidential PII and financial information.

46. Defendant, in turn, stored that information in the part of Defendant's system that was ultimately affected by the Data Breach.

47. By obtaining, collecting, and storing Plaintiff's and Class Members' PII and financial information, Defendant assumed legal and equitable duties and knew or should have known that they were thereafter responsible for protecting Plaintiff's and Class Members' PII and financial information from unauthorized disclosure.

48. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and financial information.

49. Plaintiff and Class Members relied on Defendant to keep their PII and

financial information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

50. Defendant could have prevented the Data Breach, which began between October 29, 2023, and February 12, 2024, by adequately securing and encrypting and/or more securely encrypting its servers generally, as well as Plaintiff's and Class Members' PII and financial information.

51. Defendant's negligence in safeguarding Plaintiff's and Class Members' PII and financial information is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

52. Yet, despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect Plaintiff's and Class Members' PII and financial information from being compromised.

Defendant Had an Obligation to Protect the Stolen Information

53. Defendant's failure to adequately secure Plaintiff's and Class Members' sensitive data breaches duties it owes Plaintiff and Class Members under statutory and common law.

54. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce."[4]

55. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII and financial information in Defendant's possession

[4] The Federal Trade Commission (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 the FTC Act. See, e.g., *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

56. Defendant owed a duty to Plaintiff and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the PII and financial information of Plaintiff and Class Members.

57. Defendant owed a duty to Plaintiff and Class Members to design, maintain, and test its computer systems, servers, and networks to ensure that the PII and financial information was adequately secured and protected.

58. Defendant owed a duty to Plaintiff and Class Members to create and implement reasonable data security practices and procedures to protect the PII and financial information in its possession, including not sharing information with other entities who maintained sub-standard data security systems.

59. Defendant owed a duty to Plaintiff and Class Members to implement processes that would immediately detect a breach in its data security systems in a timely manner.

60. Defendant owed a duty to Plaintiff and Class Members to act upon data security warnings and alerts in a timely fashion.

61. Defendant owed a duty to Plaintiff and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII and/or financial information from theft because such an inadequacy would be a material fact in the decision to entrust this PII and/or financial information to Defendant.

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

63. Defendant owed a duty to Plaintiff and Class Members to encrypt and/or more

reliably encrypt Plaintiff's and Class Members' PII and financial information and monitor user behavior and activity in order to identify possible threats.

Value of the Relevant Sensitive Information

64. PII and financial information are valuable commodities for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites.

65. Numerous sources cite dark web pricing for stolen identity credentials; for example, personal information 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[6]; and other sources report that criminals can also purchase access to entire company data breaches from $999 to $4,995.[7]

66. Identity thieves can use PII and financial information, such as that of Plaintiff and Class Members, which Defendant failed to keep secure, to perpetrate a variety of crimes that harm victims—for instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

67. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used:

---

[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 accessed May 9, 2024).

[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 accessed May 9, 2024).

[7] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed May 9, 2024).

according to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data might 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.[8]

68. Here, Defendant knew of the importance of safeguarding PII and financial information and of the foreseeable consequences that would occur if Plaintiff's and Class Members' PII and financial information were stolen, including the significant costs that would be placed on Plaintiff and Class Members as a result of a breach of this magnitude.

69. As detailed above, Defendant is a sophisticated organization with the resources to deploy robust cybersecurity protocols. It knew, or should have known, that the development and use of such protocols were necessary to fulfill its statutory and common law duties to Plaintiff and Class Members. Therefore, its failure to do so is intentional, willful, reckless and/or grossly negligent.

70. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its network servers were protected against unauthorized intrusions; (ii) failing to disclose that they did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' PII and financial information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

---

[8] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed May 9, 2024).

CLASS ACTION ALLEGATIONS

71. Plaintiff brings this action pursuant to the provisions of Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of herself and the following Class:

> All individuals within the United States of America whose PII and/or financial information was exposed to unauthorized third-parties as a result of the data breach experienced by Defendant between October 29, 2023 and February 12, 2024.

72. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to its departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as its immediate family members.

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

74. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of interest in the litigation, and membership in the proposed classes is easily ascertainable.

75. Numerosity: A class action is the only available method for the fair and efficient adjudication of this controversy, as the members of the Class are so numerous that joinder of all members is impractical, if not impossible.

76. Commonality: Plaintiff and the Class Members share a community of interests in that there are numerous common questions and issues of fact and law which predominate over any questions and issues solely affecting individual members, including, but not necessarily limited to:

a. Whether Defendant had a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, and/or safeguarding their PII and financial information;

b. Whether Defendant knew or should have known of the susceptibility of its data security systems and website to a data breach;

c. Whether Defendant's security procedures and practices to protect its systems and were reasonable in light of the measures recommended by data security experts;

d. Whether Defendant's failure to implement adequate data security measures allowed the Data Breach to occur;

e. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII and financial information had been compromised;

g. How and when Defendant actually learned of the Data Breach;

h. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of the PII and financial information of Plaintiff and Class Members;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and financial information of Plaintiff and Class

Members;

k. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or accounting is/are appropriate as a result of Defendant's wrongful conduct; and

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct.

77. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class sustained damages arising out of and caused by Defendant's common course of conduct in violation of law, as alleged herein.

78. Adequacy of Representation: Plaintiff in this class action is an adequate representative of the Class in that the Plaintiff has the same interest in the litigation of this case as the Class Members, is committed to the vigorous prosecution of this case and has retained competent counsel who are experienced in conducting litigation of this nature.

79. Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the class in its entirety. Plaintiff anticipates no management difficulties in this litigation.

80. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member make or may make it impractical for members of the Class to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought, by each individual member of the Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants.

81. The prosecution of separate actions would also create a risk of inconsistent rulings, which might be dispositive of the interests of the Class Members who are not parties to the adjudications and/or may substantially impede their ability to protect their interests adequately.

82. This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class in its entirety.

83. Defendant's policies and practices challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies and practices hinges on Defendant's conduct with respect to the Class in its entirety, not on facts or law applicable only to Plaintiff.

84. Unless a Class-wide injunction is issued, Defendant may continue failing to properly secure the PII and financial information of Class Members, and Defendant may continue to act unlawfully as set forth in this Complaint.

85. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

CLAIMS FOR RELIEF

COUNT ONE
Negligence
(On behalf of the Class)

86. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

87. At all times herein relevant, Defendant owed Plaintiff and Class Members a duty of

care, *inter alia*, to act with reasonable care to secure and safeguard their PII and financial information and to use commercially reasonable methods to do so. Defendant took on this obligation upon accepting and storing the PII and financial information of Plaintiff and Class Members in its computer systems and on its networks.

88. Among these duties, Defendant was expected to:

a. exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII and financial information in its possession;

b. protect Plaintiff's and Class Members' PII and financial information using reasonable and adequate security procedures and systems that were/are compliant with industry-standard practices;

c. implement processes to detect the Data Breach quickly and to timely act on warnings about data breaches; and

d. promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII and financial information.

89. Defendant knew that the PII and financial information was private and confidential and should be protected as private and confidential, and, thus, Defendant owed a duty of care not to subject Plaintiff and Class Members to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

90. Defendant knew, or should have known, of the risks inherent in collecting and storing PII and financial information, the vulnerabilities of its data security systems, and the importance of adequate security.

91. Defendant knew about numerous, well-publicized data breaches.

92. Defendant knew, or should have known, that its data systems and networks did not adequately safeguard Plaintiff's and Class Members' PII and financial information.

93. Only Defendant was in the position to ensure that its systems and protocols were sufficient to protect the PII and financial information that Plaintiff and Class Members had entrusted to it.

94. Defendant breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard their PII and financial information.

95. Because Defendant knew that a breach of its systems could damage thousands of individuals, including Plaintiff and Class Members, Defendant had a duty to adequately protect its data systems and the PII and financial information contained therein.

96. Plaintiff's and Class Members' willingness to entrust Defendant with their PII and financial information was predicated on the understanding that Defendant would take adequate security precautions.

97. Moreover, only Defendant had the ability to protect its systems and the PII and financial information stored on them from attack. Thus, Defendant had a special relationship with Plaintiff and Class Members.

98. Defendant also had independent duties under state and federal laws that required Defendant to reasonably safeguard Plaintiff's and Class Members' PII and financial information and promptly notify them about the Data Breach. These "independent duties" are untethered to any contract between Defendant, Plaintiff, and/or the remaining Class Members.

99. Defendant breached its general duty of care to Plaintiff and Class Members in the following ways, among others:

a. failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII and financial information of Plaintiff and Class Members;

b. failing to timely and accurately disclose that Plaintiff's and Class Members' PII and financial information had been improperly acquired or accessed;

c. failing to adequately protect and safeguard the PII and financial information by knowingly disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured PII and financial information;

d. failing to provide adequate supervision and oversight of the PII and financial information with which it was and is entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII and financial information of Plaintiff and Class Members, misuse the PII and intentionally disclose it to others without consent;

e. failing to adequately train its employees not to store PII and financial information longer than absolutely necessary;

f. failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class Members' PII and financial information;

g. failing to implement processes to detect data breaches, security incidents, or intrusions quickly; and

h. failing to encrypt Plaintiff's and Class Members' PII and financial information and monitor user behavior and activity in order to identify

possible threats.

100. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

101. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and Class Members have suffered damages and are at imminent risk of additional harms and damages.

102. The law further imposes an affirmative duty on Defendant to timely disclose the unauthorized access and theft of the PII and financial information to Plaintiff and Class Members so that they could and/or still can take appropriate measures to mitigate damages, protect against adverse consequences and thwart future misuse of their PII and financial information.

103. Defendant breached its duty to notify Plaintiff and Class Members of the unauthorized access by waiting months after learning of the Data Breach to notify Plaintiff and Class Members and then by failing and continuing to fail to provide Plaintiff and Class Members sufficient information regarding the breach.

104. To date, Defendant has not provided sufficient information to Plaintiff and Class Members regarding the extent of the unauthorized access and continues to breach its disclosure obligations to Plaintiff and Class Members.

105. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PII and financial information.

106. There is a close causal connection between Defendant's failure to implement security measures to protect the PII and financial information of Plaintiff and Class Members and the harm suffered, or risk of imminent harm suffered, by Plaintiff and Class Members.

107. Plaintiff's and Class Members' PII and financial information was accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII and financial information by adopting, implementing, and maintaining appropriate security measures.

108. Defendant's wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

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

110. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII and financial information is used; (iii) the compromise, publication, and/or theft of their PII and financial information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and financial 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 embarrassment and identity theft; (vi) the continued risk to their PII and financial information, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII and financial 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 PII and financial information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

111. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

112. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiff and Class Members have suffered and will suffer the continued risks of exposure of their PII and financial information, which remain in Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and financial information in its continued possession.

COUNT TWO
Breach of Implied Contract
(On behalf of the Class)

113. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

114. Through its course of conduct, Defendant, Plaintiff and Class Members entered into implied contracts for Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiff's and Class Members' PII and financial information.

115. Defendant required Plaintiff and Class Members to provide and entrust their PII and financial information as a condition of obtaining Defendant's services.

116. Defendant solicited and invited Plaintiff and Class Members to provide their PII and financial information as part of Defendant's regular business practices.

117. Plaintiff and Class Members accepted Defendant's offers and provided their PII and financial information to Defendant.

118. As a condition of their relationship with Defendant, Plaintiff and Class Members

provided and entrusted their PII and financial information to Defendant.

119. In so doing, Plaintiff and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such non-public information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and Class Members if their data had been breached and compromised or stolen.

120. A meeting of the minds occurred when Plaintiff and Class Members agreed to, and did, provide their PII and financial information to Defendant, in exchange for, amongst other things, the protection of their PII and financial information.

121. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

122. Defendant breached its implied contracts with Plaintiff and Class Members by failing to safeguard and protect their PII and financial information and by failing to provide timely and accurate notice to them that their PII and financial information was compromised as a result of the Data Breach.

123. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and Class Members have suffered (and will continue to suffer) (a) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (b) actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; (c) loss of the confidentiality of the stolen confidential data; (d) the illegal sale of the compromised data on the dark web; (e) lost work time; and (f) other economic and non-economic harm.

COUNT THREE
Breach of the Implied Covenant of Good Faith and Fair Dealing
(On behalf of the Class)

124. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

125. Every contract in this Commonwealth has an implied covenant of good faith and fair dealing, which is an independent duty and may be breached even when there is no breach of a contract's actual and/or express terms.

126. Plaintiff and Class Members have complied with and performed all conditions of their contracts with Defendant.

127. Defendant breached the implied covenant of good faith and fair dealing by failing to maintain adequate computer systems and data security practices to safeguard PII and financial information, failing to timely and accurately disclose the Data Breach to Plaintiff and Class Members and continued acceptance of PII and financial information and storage of other personal information after Defendant knew, or should have known, of the security vulnerabilities of the systems that were exploited in the Data Breach.

128. Defendant acted in bad faith and/or with malicious motive in denying Plaintiff and Class Members the full benefit of their bargains as originally intended by the parties, thereby causing them injury in an amount to be determined at trial.

COUNT FOUR
Unjust Enrichment
(On behalf of the Class)

129. Plaintiff realleges and reincorporates every allegation set forth in the preceding paragraphs as though fully set forth herein.

130. By its wrongful acts and omissions described herein, Defendant has obtained a benefit by unduly taking advantage of Plaintiff and Class Members.

131. Defendant, prior to and at the time Plaintiff and Class Members entrusted their PII and financial information to Defendant, caused Plaintiff and Class Members to reasonably believe that Defendant would keep such PII and financial information secure.

132. Defendant was aware, or should have been aware, that reasonable patients and consumers would have wanted their PII and financial information kept secure and would not have contracted with Defendant, directly or indirectly, had they known that Defendant's information systems were sub-standard for that purpose.

133. Defendant was also aware that, if the substandard condition of and vulnerabilities in its information systems were disclosed, it would negatively affect Plaintiff's and Class Members' decisions to seek services therefrom.

134. Defendant failed to disclose facts pertaining to its substandard information systems, defects, and vulnerabilities therein before Plaintiff and Class Members made their decisions to make purchases, engage in commerce therewith, and seek services or information.

135. Instead, Defendant suppressed and concealed such information. By concealing and suppressing that information, Defendant denied Plaintiff and Class Members the ability to make a rational and informed purchasing and servicing decision and took undue advantage of Plaintiff and Class Members.

136. Defendant was unjustly enriched at the expense of Plaintiff and Class Members, as Defendant received profits, benefits, and compensation, in part, at the expense of Plaintiff and Class Members; however, Plaintiff and Class Members did not receive the benefit of their bargain because they paid for products and or services that did not satisfy the purposes for which they bought/sought them.

137. Since Defendant's profits, benefits, and other compensation were obtained

improperly, Defendant is not legally or equitably entitled to retain any of the benefits, compensation or profits it realized from these transactions.

138. Plaintiff and Class Members seek an Order of this Court requiring Defendant to refund, disgorge, and pay as restitution any profits, benefits and other compensation obtained by Defendant from its wrongful conduct and/or the establishment of a constructive trust from which Plaintiff and Class Members may seek restitution.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and each member of the proposed Class, respectfully request that the Court enter judgment in their favor and for the following specific relief against Defendant as follows:

1. That the Court declare, adjudge, and decree that this action is a proper class action and certify the proposed class under F.R.C.P. Rule 23 (b)(1), (b)(2), and/or (b)(3), including the appointment of Plaintiff's counsel as Class Counsel;

2. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

3. That the Court enjoin Defendant, ordering them to cease from unlawful activities;

4. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

5. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an Order:

a. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

b. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

c. requiring Defendant to delete and purge the PII of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

d. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII;

e. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems periodically;

f. prohibiting Defendant from maintaining Plaintiff's and Class Members' PII on a cloud-based database;

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

h. requiring Defendant to conduct regular database scanning and securing checks;

i. requiring Defendant to establish an information security training program

that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

j. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

k. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to monitor Defendant's networks for internal and external threats appropriately, and assess whether monitoring tools are properly configured, tested, and updated; and

l. requiring Defendant to meaningfully educate all Class Members about the threats they face due to the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;

7. For an award of attorney's fees, costs, and litigation expenses, as allowed by law; and

8. For all other Orders, findings, and determinations identified and sought in this Complaint.

JURY DEMAND

Plaintiff, individually and on behalf of the Class, hereby demands a trial by jury for all issues triable by jury.

Respectfully submitted,

Dated: May 9, 2024

/s/ Gary F. Lynch
Gary F. Lynch (PA ID No. 56887)
Connor P. Hayes (PA ID No. 330447)
Lucia S. Romani (PA ID No. 334372)
LYNCH CARPENTER LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222
Telephone: (412) 322-9243
gary@lcllp.com
connorh@lcllp.com
lucia@lcllp.com

Kevin Laukaitis (PA ID No. 321670)
LAUKAITIS LAW LLC
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

Attorneys for Plaintiff and the Class