UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

ROBIN SUAREZ, individually and on behalf of all others similarly situated, Plaintiff, v. THE UNIVERSITY OF MASSACHUSETTS CHAN MEDICAL SCHOOL, Defendant.	Civil Action No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Robin Suarez ("Plaintiff") brings this action on behalf of herself and all others similarly situated against Defendant The University of Massachusetts Chan Medical School ("Defendant"). Plaintiff makes the following allegations pursuant to the investigation of her counsel and based upon information and belief, except as to the allegations specifically pertaining to herself, which are based on personal knowledge.

NATURE OF THE CASE

1. Plaintiff brings this action against Defendant as a result of Defendant's failure to safeguard and protect the confidential information of Plaintiff and the other members of the Class — including Social Security Numbers, Financial or Bank Account Numbers including passwords and Routing Numbers, Medicare/Medicaid Numbers, Dates of Birth, Health Insurance Policy or Subscriber Numbers, and personal information that can be used to perpetrate identity theft — in Defendant's custody, control, and care (the "Sensitive Information").

2. Defendant provides services to the Massachusetts Executive Office of Health and Human Services ("EOHHS"). Agencies and programs within EOHHS include MassHealth, the State Supplement Program, the Executive Office of Elder Affairs, and Family Resource Centers

(collectively, "the Massachusetts Public Assistance Programs").

3. Plaintiff receives services from one or more of the Massachusetts Public Assistance Programs. As a result, Defendant received Sensitive Information from Plaintiff, including, but not limited, to her Social Security Number, date of birth, financial information, Medicare/Medicaid Number, Health Insurance Policy or Subscriber Number, and other personal private data.

4. Unbeknownst to Plaintiff, Defendant did not have sufficient cyber-security procedures and policies in place to safeguard the Sensitive Information it possessed. Indeed, Defendant disclosed Plaintiff's and Class Members' Sensitive Information to a third-party, Progress Software, which had a security vulnerability in its MOVEit File Transfer solution, a system which was used by Defendant. As a result, cybercriminals were able to gain access to University of Massachusetts data, including Plaintiff and Class Members' Sensitive Information, between May 27, 2023 and May 28, 2023, thereby gaining access to approximately 134,000 Class Members' Sensitive Information, including Plaintiff's (the "Data Breach"). Plaintiff and members of the proposed Class have suffered damages as a result of the unauthorized and preventable disclosure of their Sensitive Information. Indeed, following the Data Breach, Plaintiff experienced an attempted fraud issue with her debit card.

5. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cybersecurity protections and protocols that were necessary to protect the Sensitive Information of individuals entrusted into Defendant's custody and care.

6. This lawsuit seeks to redress Defendant's unlawful disclosure of the Sensitive Information of all persons affected by this Data Breach.

PARTIES

Plaintiff Suarez

7. Plaintiff Suarez is and was a resident of Boston, Massachusetts, whose Sensitive Information was compromised in the Data Breach.

8. The Data Breach occurred between May 27, 2023 and May 28, 2023.

9. Defendant was notified of the Data Breach on June 1, 2023.

10. Defendant did not send out a notification letter, or otherwise notify Plaintiff Suarez that her Sensitive Information had been compromised, until August 14, 2023.

11. The notification letter from Defendant stated that Plaintiff Suarez's Sensitive Information, including her Social Security Number, Financial or Bank Account Number including password and Routing Number, Medicare/Medicaid Number, Date of Birth, and Health Insurance Policy or Subscriber Number, may have been compromised as a result of the Data Breach.

12. On September 6, 2023, Plaintiff Suarez was notified of a fraud issue with her debit card. Specifically, a criminal attempted to use Plaintiff Suarez's debit card at a restaurant, without Plaintiff Suarez's knowledge or consent.

Defendant

13. Defendant The University of Massachusetts Chan Medical School, is a Massachusetts-based medical school with its principal place of business located at 55 Lake Avenue North, Worcester, Massachusetts, 01655.

JURISDICTION AND VENUE

14. The Court has jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005, because at least one member of the Class,

as defined below, is a citizen of a different state than Defendant, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000 exclusive of interest and costs.

15. This Court has personal jurisdiction over Defendant because the wrongful conduct giving rise to this case occurred in, was directed to, and/or emanated from this District, and because a substantial portion of the events giving rise to Plaintiff's claims occurred in this District, including Plaintiff's provision of her Sensitive Information to Defendant.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to this claim occurred in this District, and Defendant has harmed Class Members residing in this District.

FACTUAL ALLEGATIONS

The Risks of Data Breaches and Compromised Sensitive Information are Well Known

17. Defendant had obligations created by industry standards and common law to keep Plaintiff's and Class Members' Sensitive Information confidential and to protect it from unauthorized access and disclosure.

18. Defendant's data security obligations are and were particularly important given the substantial increase in cyberattacks and/or data breaches widely reported on in the last few years. In fact, in the wake of this rise in data breaches, the Federal Trade Commission has issued an abundance of guidance for companies and institutions that maintain individuals' Sensitive Information.[1]

19. Therefore, Defendant knew or should have known of the risks of data breaches

[1] *See, e.g.*, *Protecting Personal Information: A Guide for Business,* FTC, *available at* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited Sept. 13, 2023).

and thus should have ensured that adequate protections were in place.

Defendant Allowed Criminals to Obtain Plaintiff's and the Class' Sensitive Information

20. Plaintiff and Class Members were obligated to provide Defendant with their Sensitive Information as part of their relationships, direct or indirect, with Defendant.

21. Due to inadequate security against unauthorized intrusion, including but not limited to Defendant's disclosure of Plaintiff's and Class Members' Sensitive Information to a third-party, cybercriminals breached Plaintiff's and the Class' Sensitive Information on or about May 27-28, 2023. This Data Breach resulted in the criminals unlawfully obtaining access to Plaintiff's and the Class' Sensitive Information, including their identities, Social Security Numbers, Financial or Bank Account Numbers including password and Routing Number, Medicare/Medicaid Number, Date of Birth, and Health Insurance Policy or Subscriber Number.

Data Breaches Lead to Identity Theft

22. Data breaches are more than just technical violations of their victims' rights. By accessing a victim's personal information, the cybercriminal can ransack the victim's life: withdraw funds from bank accounts, get new credit cards or loans in the victims' name, lock the victim out of his or her financial or social media accounts, send out fraudulent communications masquerading as the victim, file false tax returns, destroy their credit rating, and more.

23. Plaintiff has already been the victim of attempted fraud following the Data Breach.

24. As the United States Government Accountability Office noted in a June 2007 report on data breaches ("GAO Report"), identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits, and incur charges

and credit in a person's name.[2] As the GAO Report states, this type of identity theft is more harmful than any other because it often takes time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

25. In addition, the GAO Report states that victims of this type of identity theft will face "substantial costs and inconvenience repairing damage to their credit records."[3]

26. Identity theft victims are frequently required to spend many hours and large sums of money repairing the adverse impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phones or utilities fraud, and bank/finance fraud.

27. There may be a time lag between when sensitive information is stolen and when it is used. According to the GAO Report:

> [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.[4]

28. With access to an individual's Sensitive Information, cyber criminals can do more than just empty a victim's bank account – they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and Social Security Number to obtain government benefits; or

---

[2] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent is Unknown* (June 2007), United States Government Accountability Office, *available at* https://www.gao.gov/products/gao-07-737 (last visited Sept. 13, 2023).

[3] *Id.* at 9.

[4] *Id.* at 29

filing a fraudulent tax return using the victim's information.

29. Such personal information is such a crucial commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, Social Security Numbers, and other Sensitive Information directly on various Internet websites making the information publicly available.

30. On or about August 14, 2023, Defendant sent letters to Plaintiff and other Class members advising them that their Sensitive Information had been subject to unauthorized access and had been compromised on or about May 27-28, 2023 (the "Letter Notification"). The Letter Notification offered only five years of credit monitoring and insurance services.

Defendant's Obligations and Its Negligent Failure to Meet Them

31. In the ordinary course of using the Massachusetts Public Assistance Programs, Plaintiff, like thousands of other individuals, provided Sensitive Information, including but not limited to her Social Security Number, Financial or Bank Account Number including password and Routing Number, Medicare/Medicaid Number, Date of Birth, and Health Insurance Policy or Subscriber Number, to Defendant.

32. Defendant maintains this Sensitive Information within its data infrastructure, including within third-party vendors' systems as a result of Defendant's disclosures to said third-parties such as Progress Software.

33. Furthermore, upon information and belief, Defendant made promises and representations to the recipients of the Programs, including Plaintiff and Class Members, that the Sensitive Information collected from them as a condition of utilizing public assistance programs

would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

34. Indeed, Defendant's Privacy Statement provides that: "[w]e use computer safeguards, including multifactor authentication, to protect your information."[5]

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

36. Defendant compounded the actual and potential harm arising from the Data Breach by not fully notifying Plaintiff and other Class Members of the extent of the compromise of their personal information until August 14, 2023, when the Letter Notification was sent. Defendant's delay in notifying Plaintiff and the Class the full extent to which they were victims of the Data Breach will dilute any salutary effect that might come from these suggestions.

37. Defendant's security failure demonstrates that it failed to honor its duties by not:

(a) Maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks;

(b) Adequately protecting Plaintiff's and the Class Members' Sensitive Information;

(c) Abiding by its own stated policies and procedures with respect to Sensitive Information;

(d) Properly monitoring its own data security systems for existing intrusions; and

(e) Ensuring that agents, employees, and others with access to Sensitive Information

[5] https://www.umassmed.edu/about/privacy-statement/ (last accessed Sept. 13, 2023).

employed reasonable security procedures.

38. Plaintiff and all members of the Class have consequently suffered harm by virtue of the compromise and exposure of their Sensitive Information – including, but not limited to, (i) an imminent risk of future identity theft; (ii) lost time and money expended to mitigate the threat of identity theft; (iii) diminished value of personal information; and (iv) loss of privacy. Plaintiff and all members of the proposed Class are and will continue to be at imminent risk for tax fraud and identity theft and the attendant dangers thereof for the rest of their lives because their Sensitive Information, including Social Security Numbers, is in the hands of cyber-criminals.

Defendant's Inadequate Response to the Data Breach

39. Defendant's Letter Notification stated that it "implemented all publicly available software fixes for the MOVEit application, and [] have taken steps to monitor our vendors' data security practices more closely." No details were provided, and thus it cannot be determined from the Letter Notification whether Defendant did any of the foregoing, or if it did, whether these enhancements are sufficient to prevent recurrences similar to the Data Breach.

40. The belated Letter Notification also included an offer from Defendant of five years of free credit monitoring and identity theft resolution services through a third-party provider, Experian. Five years of credit monitoring services is insufficient, however, given that Plaintiff's and the Class Members' risk of identity theft will continue throughout their lives.

41. Conspicuously absent from the Letter Notification is any offer of compensation for out-of-pocket losses which the Class has and foreseeably will sustain – including, but not limited to, time spent to rectify any and all harms that resulted from the Data Breach. Plaintiff and members of the Class have suffered financial loss, including but not limited to lost opportunity costs for the time and effort necessary to remedy the harm they suffered. Thus,

Defendant's offer in the Letter Notification fails to make Plaintiff and the other members of the Class whole.

CLASS ALLEGATIONS

42. Plaintiff seeks to represent a class defined as:

> All persons whose Sensitive Information, provided to Defendant, was exposed to unauthorized access by way of the data breach on or about May 27-28, 2023. (Hereinafter, the "Class").

43. Plaintiff reserves the right to amend the above definition, or to propose other or additional classes, in subsequent pleadings and/or motions for class certification.

44. Plaintiff is a member of the Class.

45. Excluded from the Class are: (i) Defendant; any entity in which Defendant has a controlling interest; the officers and directors of Defendant; and the legal representatives, heirs, successors, and assigns of Defendant; (ii) any judge assigned to hear this case (or any spouse or family member of any assigned judge); (iii) any juror selected to hear this case; and (iv) any and all legal representatives (and their employees) of the parties.

46. This action seeks both injunctive relief and damages.

47. Plaintiff and the Class satisfy the requirements for class certification for the following reasons:

48. **Numerosity of the Class.** According to contemporaneous reporting of the Data Breach, the Data Breach affected approximately 134,000 individuals.[6] Therefore, the members of the Class are so numerous that their individual joinder is impracticable. The precise number of persons in the Class and their identities and addresses may be ascertained or corroborated

[6] *See* https://www.cbsnews.com/boston/news/umass-chan-data-breach-massachusetts-moveit/ (last visited Sept. 6, 2023).

from Defendant's records. If deemed necessary by the Court, members of the Class may be notified of the pendency of this action.

49. **Existence and Predominance of Common Questions of Law and Fact.** There are question of law and fact common to the Class that predominate over any questions affecting only individual members, including:

(a) Whether Defendant's data security systems prior to the Data Breach met the requirements of relevant laws;

(b) Whether Defendant's data security systems prior to the Data Breach met industry standards;

(c) Whether Plaintiff's and other Class Members' Sensitive Information was compromised in the Data Breach; and

(d) Whether Plaintiff and other Class Members are entitled to damages as a result of Defendant's conduct.

50. **Typicality.** The claims or defenses of Plaintiff are typical of the claims or defenses of the proposed Class because Plaintiff's claims are based upon the same legal theories and same violations of law. Plaintiff's grievances, like the proposed Class Members' grievances, all arise out of the same business practices and course of conduct by Defendant.

51. **Adequacy.** Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff has retained counsel that is highly experienced in complex class action litigation, and Plaintiff intends to vigorously prosecute this action on behalf of the Class. Furthermore, Plaintiff has no interests that are antagonistic to those of the Class.

52. **Superiority.** A class action is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered

by individual Class members are relatively small compared to the burden and expense of individual litigation of their claims against Defendant. It would, thus, be virtually impossible for the Class to obtain effective redress on an individual basis for the wrongs committed against them. Furthermore, even if Class members could afford such individualized litigation, the court system could not. Individualized litigation would create the danger of inconsistent or contradictory judgments arising from the same set of facts. Individualized litigation would also increase the delay and expense to all parties and the court system from the issues raised by this action. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, economies of scale, and comprehensive supervision by a single court, and presents no unusual management difficulties under the circumstances.

53. In the alternative, the Class may also be certified because:

(a) The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for the Defendant;

(b) The prosecution of separate actions by individual Class members would create a risk of adjudications with respect to them that would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; and/or

(c) Defendant has acted or refused to act on grounds generally applicable to the Class as a whole, thereby making appropriate final declaratory and/or injunctive relief with respect to the members of the Class as a whole.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

54. Plaintiff hereby incorporates by reference the allegations contained in all preceding paragraphs of this complaint.

55. Defendant owed a duty to Plaintiff and to the Class to exercise reasonable care in obtaining, securing, safeguarding, properly disposing of and protecting Plaintiff's and Class Members' Sensitive Information within its control from being compromised, including by being accessed by unauthorized third parties. This duty included, among other things, maintaining adequate security measures over its networks and systems — including third parties it disclosed the Sensitive Information to — so as to prevent unauthorized access thereof.

56. Defendant owed a duty of care to the Plaintiff and members of the Class to provide security, consistent with industry standards, to ensure that it adequately protected the Sensitive Information of the individuals who entrusted it to Defendant.

57. Only Defendant was in a position to ensure that its and its vendors' systems were sufficient to protect against the harm to Plaintiff and the members of the Class from the Data Breach.

58. In addition, Defendant had a duty to use reasonable security measures under Section A 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.

59. Defendant's duty to use reasonable care in protecting the Sensitive Information arose not only as a result of the common law and the statutes and regulations described above, but also because they are bound by, and have committed to comply with, industry standards for

the protection of confidential information, as well as its own stated policies.

60. Defendant breached its common law, statutory, and other duties – and thus, was negligent – by failing to use reasonable measures to protect Plaintiff and Class Members' Sensitive Information, and by failing to provide timely notice of the Data Breach, and/or by failing to abide by its own stated policies. 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 security measures to safeguard Plaintiff's and the Class members' Sensitive Information;

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

(c) Failing to abide by its own stated policies with respect to Plaintiff's and the Class Members' Sensitive Information;

(d) Allowing unauthorized access to Plaintiff's and the Class Members' Sensitive Information; and

(e) Failing to warn Plaintiff and other Class Members about the full extent of the Data Breach in a timely manner so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

61. Defendant owed a duty of care to the Plaintiff and the members of the Class because they were foreseeable and probable victims of any inadequate security practices.

62. It was foreseeable that Defendant's failure to use reasonable measures to protect Sensitive Information and to provide timely notice of the full extent of the Data Breach would result in injury to Plaintiff and other Class Members. Further, the breach of security, unauthorized access, and resulting injury to Plaintiff and the members of the Class were reasonably foreseeable.

63. It was therefore foreseeable that the failure to adequately safeguard Sensitive Information would result in one or more of the following injuries to Plaintiff and the members of the Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of confidentiality of the stolen confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

64. Defendant knew or reasonably should have known of the inherent risks in collecting and storing the Sensitive Information of Plaintiff and members of the Class and the critical importance of providing adequate security of that information, yet despite the foregoing had inadequate cyber-security systems and protocols in place to secure the Sensitive Information.

65. As a result of the foregoing, Defendant unlawfully breached its duty to use reasonable care to protect and secure the Sensitive Information of Plaintiff and the Class which Plaintiff and members of the Class were required to provide to Defendant.

66. Plaintiff and members of the Class reasonably relied on Defendant to safeguard their information, and while Defendant was in a position to protect against harm from a data breach, Defendant negligently and carelessly squandered that opportunity. As a proximate result, Plaintiff and members of the Class suffered and continue to suffer the consequences of the Data breach.

67. Defendant's negligence was the proximate cause of harm to Plaintiff and

members of the Class.

68. Had Defendant not failed to implement and maintain adequate security measures to protect the Sensitive Information, the Plaintiff's and Class Members' Sensitive Information would not have been exposed to unauthorized access and stolen, and they would not have suffered any harm.

69. However, as a direct and proximate result of Defendant's negligence, Plaintiff and members of the Class have been seriously and permanently damaged by the Data Breach. Specifically, Plaintiff and members of the Class have been injured by, among other things; (1) the loss of opportunity to control how their Sensitive Information is used; (2) diminution of value and the use of their Sensitive Information; (3) compromise, publication and/or theft of the Plaintiff's and the Class Members' Sensitive Information; (4) out-of-pocket costs associated with the prevention, detection and recovery from identity theft and/or unauthorized use of financial accounts; (5) lost opportunity costs associated with their efforts expended and the loss of productivity from addressing as well as attempting to mitigate the actual and future consequences of the breach including, but not limited to, efforts spent researching how to prevent, detect, and recover from identity data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased cost of the use, the use of credit, credit scores, credit reports, and assets; (7) unauthorized use of compromised Sensitive Information to open new financial accounts; (8) tax fraud and/or other unauthorized charges to financial accounts and associated lack of access to funds while proper information is confirmed and corrected and/or imminent risk of the foregoing; (9) continued risks to their Sensitive Information, which remains in Defendant's possession and may be subject to further breaches so long as Defendant fails to undertake

appropriate and adequate measures to protect the Sensitive Information in its possession; and (10) future costs in terms of time, effort and money that will be spent trying to prevent, detect, contest and repair the effects of the Sensitive Information compromised as a result of the Data Breach as a remainder of the Plaintiff's and Class Members' lives.

70. Plaintiff and the Class seek damages, injunctive relief, and other and further relief as the Court may deem just and proper.

COUNT II
Breach Of Third-Party Beneficiary Contract
(On Behalf of Plaintiff and the Class)

71. Plaintiff hereby incorporates by reference the allegations contained in all preceding paragraphs of this complaint.

72. Defendant entered into written contracts, with its clients, including the Massachusetts Public Assistance Programs, to provide services.

73. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the Sensitive Information of Plaintiff and the Class and to timely and adequately notify them of the Data Breach.

74. These contracts were made expressly for the benefit of Plaintiff and the Class, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered into between Defendant and the Massachusetts Public Assistance Programs. Defendant knew that, if it were to breach these contracts with the Massachusetts Public Assistance Programs, the Massachusetts Public Assistance Programs' plan members and/or beneficiaries—Plaintiff and Class Members—would be harmed.

75. Defendant breached the contracts it entered into with the Massachusetts Public Assistance Programs by, among other things, failing to (i) use reasonable data security measures,

(ii) implement adequate protocols and employee training sufficient to protect Plaintiff's Sensitive Information from unauthorized disclosure to third parties, and (iii) promptly and adequately notify Plaintiff and Class Members of the Data Breach.

76. Plaintiff and the Class were harmed by Defendant's breach of its contracts with the Massachusetts Public Assistance Programs, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

77. Plaintiff and Class Members are also entitled to their costs and attorney's fees incurred in this action.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

78. Plaintiff hereby incorporates by reference the allegations contained in all preceding paragraphs of this complaint.

79. Plaintiff and Class Members conferred a monetary benefit on Defendant. Specifically, they provided their valuable Sensitive Information, directly or indirectly, to Defendant and/or its agents. In exchange, Plaintiff and Class Members should have received from Defendant the services that were the subject of the transaction and should have had their Sensitive Information protected with adequate data security.

80. Defendant knew that Plaintiff and Class Members conferred a benefit on it in the form of their Sensitive Information as well as payments made on their behalf as a necessary part of receiving benefits and/or services through the Massachusetts Public Assistance Programs. Defendant appreciated and accepted that benefit. Defendant profited from these transactions and used the Senestivie Information of Plaintiff and Class Members for business purposes.

81. Upon information and belief, Defendant funds its data security measures entirely

from its general revenue, including payments on behalf of or for the benefit of Plaintiff and Class Members.

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

83. Defendant, however, failed to secure Plaintiff's and Class Members' Sensitive Information and, therefore, did not provide adequate data security in return for the benefit Plaintiff and Class Members provided.

84. Defendant would not be able to carry out an essential function of its regular business without the Sensitive Information of Plaintiff and Class Members and derived revenue by using it for business purposes. Plaintiff and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

85. Defendant acquired the Sensitive Information through inequitable means in that it failed to investigate and/or disclose the inadequate security practices previously alleged.

86. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Sensitive Information, they would not have allowed their Sensitive Information to be provided to Defendant.

87. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiff and Class

Members by utilizing cheaper, ineffective security measures and diverting those funds to its won profit. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Sensitive Information.

88. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained from Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

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

90. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

91. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

PRAYER FOR RELIEF

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

(a) For an order certifying the Class under Rule 23 of the Federal Rules of Civil Procedure and naming Plaintiff as a representative of the Class and Plaintiff's attorneys as Class Counsel to represent the Class;

(b) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;

(c) For compensatory and punitive damages in amounts to be determined by the Court and/or jury;

(d) For prejudgment interest on all amounts awarded;

(e) For an order of restitution and all other forms of equitable monetary relief;

(f) For an order directing Defendant to cease the illegal actions detailed herein; and

(g) For an order awarding Plaintiff and the Class their reasonable attorneys' fees and expenses and costs of suit.

DEMAND FOR TRIAL BY JURY

Plaintiff, individually and on behalf of the Class, demands a trial by jury as to all issues triable of right.

Dated: September 18, 2023

Respectfully submitted,

BURSOR & FISHER, P.A.

By: */s/Joel. D. Smith*

Joel D. Smith (BBO 712418)
L. Timothy Fisher (*pro hac vice* forthcoming)
1990 North California Boulevard, Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
Email: jsmith@bursor.com
ltfisher@bursor.com

BURSOR & FISHER, P.A.
Matthew A. Girardi (*pro hac vice* forthcoming)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
Email: mgirardi@bursor.com

Counsel for Plaintiff