UNITED STATES DISTRICT COURT
DISTRICT OF NEBRASKA

KENNEDY FREEMAN, and AARON MORRIS, Individually, and on Behalf of All Others Similarly Situated, Plaintiff, v. NELNET SERVICING, LLC, Defendant.	Case No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Kennedy Freeman and Aaron Morris ("Plaintiffs"), through their undersigned counsel, bring this action against Nelnet Servicing, LLC. ("Nelnet" or "Defendant") pursuant to the investigation of their attorneys, personal knowledge as to themselves and their own acts and otherwise upon information and belief, and allege as follows:

INTRODUCTION

1. Nelnet provides technology and web-based services to student loan servicers, most notably for the context of this complaint, the Oklahoma Student Loan Authority ("OSLA") and Edfinancial Services, LLC ("Edfinancial").

2. On or about August 26, 2022, Nelnet began publicly acknowledging and writing to affected persons that it had been the recipient of a hack and exfiltration of personally identifiable information ("PII"), including sensitive personal information ("SPI") such as Social Security numbers, involving more than 2,500,000 individuals whose student loans are serviced by Nelnet's customers (the "Data Breach").

3. Notably, Nelnet did not appear to report exactly when the Data Breach occurred other than noting that it possibly occurred in June or July 2022. It began to notify its clients OSLA and Edfinancial of the Data Breach on or around July 21, 2022.

4. Nelnet reported that this PII included Social Security numbers, names, addresses, email addresses, and telephone numbers, allowing Social Security Numbers to be matched to individuals with great specificity.

5. Plaintiff and Class members now face a present and imminent lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

6. The information stolen in cyber-attacks allows the modern thief to assume victims' identities when carrying out criminal acts such as:

- Filing fraudulent tax returns;
- Using a victim's credit history;
- Making financial transactions on behalf of victims, including opening credit accounts in victims' names;
- Impersonating victims via mail and/or email;
- Impersonating victims in cyber forums and social networks;
- Stealing benefits that belong to victims; and
- Committing illegal acts which, in turn, incriminate victims.

7. Plaintiffs' and Class members' PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiffs and Class members.

8. As of this writing, there exist many Class members who have no idea their PII has been compromised and that they are at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes. Nelnet has not publicly posted information about the data breach on its website, and neither have OSLA

or Edfinancial.

9. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect consumers' PII, (ii) adequately warn its current and former customers and potential customers of its inadequate information security practices, and (iii) effectively monitor its platforms for security vulnerabilities and incidents (the "Class"). Defendant's conduct amounts to negligence and violates state statutes.

10. Plaintiffs and similarly situated individuals have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished inherent value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) deprivation of rights they possess under state and federal data privacy laws; and (v) the continued and certainly an increased risk to their PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

12. This Court has personal jurisdiction over Defendant because Defendant's principal places of business is located within this District and Defendant conducts substantial business in Nebraska and this District through its headquarters, offices, parents, and affiliates.

13. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial District.

PARTIES

14. Plaintiff Kennedy Freeman is a natural person residing in Dallas, Texas. On or about August 28, 2022, Plaintiff Freeman was informed via letter dated August 26, 2022 that she had been a victim of the Data Breach.

15. Plaintiff Aaron Morris is a natural person residing in Bend, Oregon. On or about August 31, 2022, Plaintiff Morris was informed via letter dated August 26, 2022 that he had been a victim of the Data Breach.

16. Defendant Nelnet Servicing, LLC is a Nebraska limited liability corporation with its principal place of business at 121 S. 13th Street, Suite 100 Lincoln, Nebraska 68508.

FACTUAL ALLEGATIONS

17. Defendant is a provider of technology and web-based services to federal student loan servicers, notably, for the purposes of this Complaint, OSLA and Edfinancial.

18. In the normal course of business, Nelnet collects PII from individuals whose loans are serviced by companies such as OSLA and Edfinancial. This PII specifically includes Social Security Numbers, and when combined with names, email addresses, addresses, and phone numbers, such as those lost in the Data Breach, it gives hackers the ability to clear match Social Security Numbers to individuals.

19. Nelnet's Privacy Policy states, "Nelnet takes careful steps to safeguard customer information. We restrict access to your personal and account information to employees who need to know the information to provide services to you, and we regularly train our employees on privacy, information security, and their obligation to protect your information. We maintain reasonable and appropriate physical, electronic, and procedural safeguards to guard your

Nonpublic Personal Information (NPI) and Personally Identifiable Information (PII), and we regularly test those safeguards to maintain the appropriate levels of protection."[1]

20. On or about August 26, 2022, Defendant announced publicly that on July 21, 2021 it "notified Edfinancial and OSLA that it had discovered a vulnerability it believed led to this incident. Nelnet Servicing informed Edfinancial and OSLA that Nelnet Servicing's cybersecurity team took immediate action to secure the information system, block the suspicious activity, fix the issue, and launched an investigation with third-party forensic experts to determine the nature and scope of the activity."[2]

21. Nelnet further stated, "On August 17, 2022, this investigation determined that certain student loan account registration information was accessible by an unknown party beginning in June 2022 and ending on July 22, 2022."[3]

22. Of concern, Nelnet has provided no greater clarity regarding the nature of the access, the exact date of the breach, or whether SPI beyond Social Security Numbers may have been implicated.

23. While the Data Breach was reported in security websites at the time, there appears to have been no wide-scale press release regarding the Data Breach, and neither Defendant nor OSLA or Edfinancial appear to have posted information about the breach on their websites.

24. As a result, Plaintiffs' and Class members' PII was in the hands of hackers for at least two months before Defendant began notifying them of the Data Breach.

---

[1] https://www.nelnet.com/privacy-and-security (last accessed September 6, 2022).
[2] https://apps.web.maine.gov/online/aeviewer/ME/40/f6b4d5be-f7ef-412b-9966-e323ad6443a0/a3db2f97-5a75-4217-9982-873343015f4b/document.html (last accessed September 6, 2022).
[3] *Id.*

25. Defendant has been vague on its response to the Data Breach, stating that "Nelnet Servicing moved quickly to investigate and respond to the incident, assess the security of Nelnet Servicing systems, notify Edfinancial and OSLA, and identify potentially affected individuals. Further, Nelnet Servicing notified federal law enforcement regarding the event."[4]

26. As of this writing, Defendant has offered no concrete information on the steps it has taken or specific efforts made to reasonably ensure that such a breach cannot or will not occur again.

27. Appallingly, Defendant is offering no additional assistance to Plaintiffs and class members beyond the entirely inadequate monitoring suggestions that are a part of its notice. Edfinancial and OSLA both state that they are offering 24 months of credit monitoring through Experian.

28. This response is entirely inadequate to Plaintiffs and Class members who now potentially face several years of heightened risk from the theft of their PII and who may have already incurred substantial out-of-pocket costs in responding to the Data Breach.

29. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

30. Furthermore, this is not Nelnet's first data breach. In 2011, a Nelnet employee was charged with using student information to fraudulently open credit cards and loans.[5]

31. Plaintiffs and Class members provided their PII to Defendant with the reasonable

---

[4] *Id.*

[5] *See* https://www.databreaches.net/nelnet-employee-accused-of-misusing-customer-info/ (last accessed September 6, 2022).

expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

32. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches preceding the date of the breach.

33. Indeed, data breaches, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry, including Defendant.

34. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[6] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[7]

35. The PII of Plaintiffs and members of the Classes was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

36. Defendant knew, or reasonably should have known, of the importance of

---

[6] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf, (last accessed September 6, 2022)

[7] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

safeguarding the PII of Plaintiffs and members of the Class, including Social Security numbers, dates of birth, and other sensitive information, as well as of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and members of the Class a result of a breach.

37. Plaintiffs and members of the Class now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

38. The injuries to Plaintiffs and members of the Class were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and members of the Class.

39. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

40. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

41. The FTC further recommends that companies not maintain PII longer than is

needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

42. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, 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 ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

43. Defendant failed to properly implement basic data security practices, and its failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

44. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices.

45. Best cybersecurity practices include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

46. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1

(including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

47. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

48. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers; they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

49. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[8]

50. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive

[8] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs (last accessed September 6, 2022).

financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[9]

51. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

52. Even then, a new Social Security number may not be effective. According to Julie Fergerson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[10]

53. Furthermore, as the SSA warns:

> Keep in mind that a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you shouldn't use the old number anymore.

---

[9] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed September 6, 2022).

[10] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015),http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed September 6, 2022)

> For some victims of identity theft, a new number actually creates new problems. If the old credit information isn't associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit.[11]

54. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential PII to mimic the identity of the user. The personal data of Plaintiffs and members of the Class stolen in the Data Breach constitutes a dream for hackers and a nightmare for Plaintiffs and the Class. Stolen personal data of Plaintiffs and members of the Class represents essentially one-stop shopping for identity thieves.

55. The FTC has released its updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

56. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional Requesters:

> [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.[12]

57. Companies recognize that PII is a valuable asset. Indeed, PII is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other PII on a number of Internet websites. The stolen personal data of Plaintiffs and members of the Class has a high value on both legitimate and black markets.

---

[11] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), http://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed September 6, 2022)

[12] *See* https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29 (last accessed September 6, 2022)

58. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

59. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Defendant's former and current customers whose Social Security numbers have been compromised now face a real, present, imminent and substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

60. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change — Social Security number, driver license number or government-issued identification number, name, and date of birth.

61. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x in price on the black market."[13]

62. This is even more true for minors, whose Social Security Numbers are particularly valuable. As one site noted, "The organization added that there is extreme credit value in Social

---

[13] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed September 6, 2022)

Security numbers that have never been used for financial purposes. It's relatively simple to add a false name, age or address to a Social Security number. After that happens, there is a window for thieves to open illicit credit cards or even sign up for government benefits."[14]

63. Among other forms of fraud, identity thieves may obtain driver licenses, government benefits, medical services, and housing or even give false information to police. An individual may not know that his or her driver license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

FACTS SPECIFIC TO PLAINTIFFS

Plaintiff Kennedy Freeman

64. Plaintiff Freeman provided her personal information to Nelnet and/or its affiliate OSLA in conjunction with servicing related to Plaintiff Freeman's student loans.

65. As part of her involvement with Defendant and OSLA, Plaintiff Freeman entrusted her PII, and other confidential information such as name, address, Social Security number, phone number, financial account information, and other personally identifiable information with the reasonable expectation and understanding that Nelnet and OSLA would take at a minimum industry standard precautions to protect, maintain, and safeguard that information from unauthorized use or disclosure, and would timely notify her of any data security incidents related to her. Plaintiff would not have permitted her PII to be given to Nelnet had she known it would not take reasonable steps to safeguard her PII.

66. On or about August 28, 2022, nearly three months after Nelnet's breach began,

---

[14] https://www.identityguard.com/news/kids-targeted-identity-theft (last accessed September 6, 2022)

Plaintiff Freeman was notified via a physical letter (dated August 26, 2022) from OSLA that her PII had been improperly accessed and taken by unauthorized third parties. The notice indicated that Plaintiff Freeman's PII was compromised as a result of the Data Breach.

67. As a result of the Data Breach, Plaintiff Freeman has or will make reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or personal records for any indications of actual or attempted identity theft or fraud.

68. Plaintiff Freeman spent this time at OSLA's direction. Indeed, in the Notice letter Plaintiff Freeman received, OSLA directed Plaintiff Freeman to take steps to mitigate her losses:

> We encourage you to remain vigilant against incidents of identity theft and fraud over the next 24 months, by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the enclosed "*Steps You Can Take to Help Protect Your Personal Information*."

69. Plaintiff Freeman suffered actual injury from having her PII compromised as a result of the Data Breach. Beginning in August, Plaintiff Freeman's credit score decreased by between approximately 20 to 40 points, depending upon the credit reporting service, due to no factors which Plaintiff Freeman has been able to determine beyond the Data Breach.

70. Additionally, Plaintiff Freeman has experienced a surge in spam calls and texts roughly coincident with the timing of the Data Breach, indicating that hackers are already trying to take advantage of the release of her PII.

71. Additionally, Plaintiff Freeman is aware of no other source from which the theft of her PII could have come. She regularly takes steps to safeguard her own PII in her own control.

72. Plaintiff Freeman has suffered other injury including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Nelnet obtained from Plaintiff Freeman; (b) violation of her privacy rights; (c) the theft of her PII; and (d) imminent and

impending injury arising from the increased risk of identity theft and fraud.

73. As a result of the Data Breach, Plaintiff Freeman is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

74. The Data Breach has caused Plaintiff Freeman to suffer significant fear, anxiety, and stress, which has been compounded by the fact that her Social Security number and other intimate details are in the hands of criminals.

75. As a result of the Data Breach, Plaintiff Freeman anticipates spending considerable time and/or money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Freeman will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

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

Plaintiff Aaron Morris

77. Plaintiff Morris provided his personal information to Nelnet and/or its affiliate Edfinancial in conjunction with servicing related to Plaintiff Morris' student loans.

78. As part of his involvement with Defendant and Edfinancial, Plaintiff Morris entrusted his PII, and other confidential information such as name, address, Social Security number, phone number, financial account information, and other personally identifiable information with the reasonable expectation and understanding that Nelnet and Edfinancial would take at a minimum industry standard precautions to protect, maintain, and safeguard that information from unauthorized use or disclosure, and would timely notify him of any data security

incidents related to him. Plaintiff Morris would not have permitted his PII to be given to Nelnet had he known it would not take reasonable steps to safeguard his PII.

79. On or about August 31, 2022, nearly three months after Nelnet's breach began, Plaintiff Morris was notified via a physical letter (dated August 26, 2022) from Edfinancial that his PII had been improperly accessed and taken by unauthorized third parties. The notice indicated the Plaintiff Morris' PII was compromised as a result of the Data Breach.

80. As a result of the Data Breach, Plaintiff Morris has or will make reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or personal records for any indications of actual or attempted identity theft or fraud.

81. Plaintiff Morris spent this time at Edfinancial's direction. Indeed, in the Notice letter Plaintiff Morris received, Edfinancial directed Plaintiff Morris to take steps to mitigate his losses:

> We encourage you to remain vigilant against incidents of identity theft and fraud over the next 24 months, by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please also review the information contained in the enclosed "*Steps You Can Take to Help Protect Your Personal Information*."

82. Plaintiff Morris suffered actual injury from having his PII compromised as a result of the Data Breach. In July of 2022, Plaintiff Morris began receiving suspicious text messages and phone calls from banks and insurance companies. On July 31, 2022, Plaintiff Morris received a text message from Keesler Federal Credit Union alerting him to suspicious activity in his account—but Plaintiff Morris does not have and never has had an account with Keesler Federal Credit Union.

83. Moreover, on or about July 26, 2022, Plaintiff Morris received a text message from Liberty Mutual regarding a quote for coverage, but Plaintiff Morris did not request a quote. One

or two other insurance companies also reached out to him via text message or phone calls within 24 hours of receiving the text message from Liberty Mutual.

84. Plaintiff Morris has suffered other injury including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Nelnet obtained from Plaintiff Morris; (b) violation of his privacy rights; (c) the theft of his PII; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

85. As a result of the Data Breach, Plaintiff Morris is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

86. The Data Breach has caused Plaintiff Morris to suffer significant fear, anxiety, and stress, which has been compounded by the fact that his Social Security number and other intimate details are in the hands of criminals.

87. As a result of the Data Breach, Plaintiff Morris anticipates spending considerable time and/or money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Morris will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

88. Plaintiff Morris has a continuing interest in ensuring that his PII, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

89. Plaintiffs bring this class action pursuant to Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following classes:

> All natural persons residing in the United States whose PII was compromised in the 2022 Data Breach announced by Defendant, Edfinancial and/or OSLA on or about August 26, 2022 (the "Class").

90. Excluded from the Class are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

91. Plaintiffs reserve the right to modify or amend the definitions of the proposed Class before the Court determines whether certification is appropriate.

92. **Numerosity**: The Classes are so numerous that joinder of all members is impracticable. One security websites has, as of this writing, indicated that the total number of Class members is approximately 2,501,324.[15] The Class is readily identifiable within Defendant's and OSLA's and Edfinancial's records.

93. **Commonality**: Questions of law and fact common to the Class exist and predominate over any questions affecting only individual members of the Class. These include:

a. When Defendant actually learned of the Data Breach and whether its response was adequate;

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

c. Whether Defendant breached that duty;

d. Whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of storing the PII of Plaintiffs and members of the Classes;

e. Whether Defendant acted negligently in connection with the monitoring and/or protection of PII belonging to Plaintiffs and members of the Class;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep the PII of Plaintiffs and members of the Class secure and to prevent loss or

---

[15] *See* https://www.bleepingcomputer.com/news/security/nelnet-servicing-breach-exposes-data-of-25m-student-loan-accounts/ (last accessed September 6, 2022)

misuse of that PII;

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

h. Whether Defendant caused Plaintiffs and members of the Class damage;

i. Whether Defendant violated the law by failing to promptly notify Plaintiffs and members of the Class that their PII had been compromised; and

j. Whether Plaintiffs and the other members of the Class are entitled to credit monitoring and other monetary relief.

94. **Typicality**: Plaintiffs' claims are typical of those of the other members of the Class because all had their PII compromised as a result of the Data Breach due to Defendant's misfeasance.

95. **Adequacy**: Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' counsel are competent and experienced in litigating privacy-related class actions.

96. **Superiority and Manageability**: Under Rule 23(b)(3) and 23(a)(1) of the Federal Rules of Civil Procedure, a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Individual damages for any individual member of the Class are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

97. Class certification is also appropriate under Rule 23(a) and (b)(2) because Defendant has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

98. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification

because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and members of the Classes to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendant breached a legal duty to Plaintiffs and the members of the Class to exercise due care in collecting, storing, using, and safeguarding their PII;

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

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether members of the Class are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

FIRST CLAIM FOR RELIEF
Negligence
(By Plaintiffs Individually and on Behalf of the Class)

99. Plaintiffs hereby re-allege and incorporate by reference all of the allegations in paragraphs 1 to 98.

100. As a condition of having their student loans processed, Plaintiffs and Class Members, as current and former student loan borrowers, are obligated to provide Nelnet and/or its affiliates with certain PII, including but not limited to, their name, date of birth, address, Social Security number, state-issued identification numbers, tax identification numbers, military identification numbers, and financial account numbers.

101. Plaintiffs and Class Members entrusted their PII to Nelnet and its affiliates on the premise and with the understanding that Nelnet would safeguard their information, use their PII for legitimate business purposes only, and/or not disclose their PII to unauthorized third parties.

102. Nelnet has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and Class Members could and would suffer if the PII were wrongfully disclosed.

103. Nelnet knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and/or using of the PII involved an unreasonable risk of harm to Plaintiffs and Class Members, even if the harm occurred through the criminal acts of a third party.

104. Nelnet had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Nelnet's security protocols to ensure that Plaintiffs' and Class Members' information in Nelnet's possession was adequately secured and protected.

105. Nelnet also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' and Class Members' PII.

106. A breach of security, unauthorized access, and resulting injury to Plaintiffs and Class Members was reasonably foreseeable, particularly in light of Nelnet's business as sophisticated student loan service provider, for which the diligent protection of PII is a continuous forefront issue.

107. Plaintiffs and Class Members were the foreseeable and probable victims of Nelnet's inadequate security practices and procedures. Nelnet knew of should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Class, the critical importance of

providing adequate security of that PII, and the necessity for encrypting PII stored on Nelnet's systems.

108. Nelnet's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Nelnet's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Nelnet's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiffs' and Class Members' PII, including basic encryption techniques freely available to Nelnet.

109. Plaintiffs and Class Members had no ability to protect their PII that was in, and possibly remains in, Nelnet's possession.

110. Nelnet was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

111. Nelnet had and continues to have a duty to adequately and promptly disclose that Plaintiffs' and Class Members' PII within Nelnet's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

112. Nelnet had a duty to employ proper procedures to prevent the unauthorized dissemination of Plaintiffs' and Class Members' PII.

113. Nelnet has admitted that the PII of Plaintiffs and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

114. Nelnet, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and Class Members by failing to implement industry protocols and exercise reasonable

care in protecting and safeguarding Plaintiffs' and Class Members' PII during the time the PII was within Nelnet's possession or control.

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

116. These foregoing frameworks are existing and applicable industry standards in the financial services industry, and Defendant failed to comply with these accepted standards thereby opening the door to the cyber incident and causing the data breach.

117. Nelnet improperly and inadequately safeguarded Plaintiffs' and Class Members' PII in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

118. Nelnet failed to heed industry warnings and alerts to provide adequate safeguards to protect borrower PII in the face of increased risk of theft.

119. Nelnet, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

120. Nelnet, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and Class Members the existence and scope of the Data Breach.

121. But for Nelnet's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, Plaintiffs' and Class Members' PII would not have been compromised.

122. There is a close causal connection between Nelnet's failure to implement security measures to protect Plaintiffs' and Class Members' PII and the harm suffered or risk of imminent harm suffered by Plaintiffs and Class. Plaintiffs' and Class Members' PII was lost and accessed as the proximate result of Nelnet's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

123. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Nelnet, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Nelnet's duty in this regard.

124. Nelnet violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Nelnet's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members.

125. Nelnet's violation of Section 5 of the FTC Act constitutes negligence per se.

126. Plaintiffs and Class members are within the class of persons that the FTC Act was intended to protect.

127. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class.

128. As a direct and proximate result of Nelnet's negligence and negligence per se, Plaintiffs 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 is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (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 tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Nelnet's possession and is subject to further unauthorized disclosures so long as Nelnet fails to undertake appropriate and adequate measures to protect the PII in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members; and (ix) the diminished value of Nelnet's goods and services they received.

129. As a direct and proximate result of Nelnet's negligence, Plaintiffs 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.

130. Additionally, as a direct and proximate result of Nelnet's negligence and negligence per se, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their PII, which remains in Nelnet's possession and is subject to further unauthorized disclosures so long as Nelnet fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

SECOND CLAIM FOR RELIEF
Unjust Enrichment

(By Plaintiffs Individually and on Behalf of the Class)

131. Plaintiffs hereby re-allege and incorporate by reference all of the allegations in paragraphs 1 to 98.

132. Plaintiffs and Class Members conferred a monetary benefit on Defendant and its affiliate student loan companies in the form of monetary payments—directly or indirectly—for providing student loan services to current and former borrowers.

133. Defendant collected, maintained, and stored the PII of Plaintiffs and Class Members and, as such, Defendant had knowledge of the monetary benefits it received on behalf of the Plaintiffs and Class Members.

134. The money that borrowers paid to Defendant should have been used to pay, at least in part, for the administrative costs and implementation of data security adequate to safeguard and protect the confidentiality of Plaintiffs' and Class Members' PII.

135. Defendant failed to implement—or adequately implement—those data security practices, procedures, and programs to secure sensitive PII, as evidenced by the Data Breach.

136. As a result of Defendant's failure to implement data security practices, procedures, and programs to secure sensitive PII, Plaintiffs and Class Members suffered actual damages in an amount of the savings and costs Defendant reasonably and contractually should have expended on data security measures to secure Plaintiffs' PII.

137. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and Class Members because Defendant failed to implement the data security measures adequate to safeguard and protect the confidentiality of Plaintiffs' and Class Members' PII and that the borrowers paid for.

138. As a direct and proximate result of Defendant's decision to profit rather than provide adequate security, and Defendant's resultant disclosures of Plaintiffs' and Class Members'

PII, Plaintiffs and Class Members suffered and continue to suffer considerable injuries in the forms of time and expenses mitigating harms, diminished value of PII, loss of privacy, and a present increased risk of harm.

THIRD CLAIM FOR RELIEF
Breach of Express Contract
(By Plaintiffs Individually and on Behalf of the Class)

139. Plaintiffs hereby re-allege and incorporate by reference all of the allegations in paragraphs 1 to 98.

140. This count is plead in the alternative to Count II (Unjust Enrichment) above.

141. Plaintiffs and Class Members allege that they were the express, foreseeable, and intended beneficiaries of valid and enforceable express contracts between Defendant and its former and current customers, contract(s) that (upon information and belief) include obligations to keep sensitive PII private and secure.

142. Upon information and belief, these contracts included promises made by Defendant that expressed and/or manifested intent that the contracts were made to primarily and directly benefit the Plaintiffs and the Class (all customers entering into the contracts), as Defendant's service was for student loan services for Plaintiffs and the Class, but also safeguarding the PII entrusted to Defendant in the process of providing these services.

143. Upon information and belief, Defendant's representations required Defendant to implement the necessary security measures to protect Plaintiffs' and Class Members' PII.

144. Defendant materially breached its contractual obligation to protect the PII of Plaintiffs and Class Members when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

145. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

146. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure of their PII, the loss of control of their PII, the present risk of suffering additional damages, and out-of-pocket expenses.

147. Plaintiffs and Class Members are entitled to compensator, consequential, and nominal damages suffered as a result of the Data Breach.

FOURTH CLAIM FOR RELIEF
Breach of Implied Contract
(By Plaintiffs Individually and on Behalf of the Class)

148. Plaintiffs hereby re-allege and incorporate by reference all of the allegations in paragraphs 1 to 98.

149. This count is plead in the alternative to Count II (Unjust Enrichment) above.

150. Plaintiffs' and Class Members' PII was provided to Defendant as part of student loan services that Defendant provided to Plaintiffs and Class Members.

151. Plaintiffs and Class Members agreed to pay Defendant for its services.

152. Defendant and the Plaintiffs and Class Members entered into implied contracts for the provision of adequate data security, separate and apart from any express contracts concerning the security of Plaintiffs' and Class Members' PII, whereby, Defendant was obligated to take reasonable steps to secure and safeguard Plaintiffs' and Class Members' PII.

153. Defendant had an implied duty of good faith to ensure that the PII of Plaintiffs and Class Members in its possession was only used in accordance with its contractual obligations.

154. Defendant was therefore required to act fairly, reasonably, and in good faith in carrying out its contractual obligations to protect the confidentiality of Plaintiffs' and Class Members' PII and to comply with industry standards and applicable laws and regulations for the security of this information.

155. Under these implied contracts for data security, Defendant was further obligated to provide Plaintiffs and all Class Members, with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII.

156. Defendant breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiffs' and Class Members' PII, resulting in the Data Breach.

157. Defendant further breached the implied contract by providing untimely notification to Plaintiffs and Class Members who may already be victims of identity fraud or theft or are at present risk of becoming victims of identity theft or fraud.

158. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

159. As a result of Defendant's conduct, Plaintiffs and Class Members did not receive the full benefit of the bargain.

160. Had Defendant disclosed that its data security was inadequate, neither the Plaintiffs or Class Members, nor any reasonable person would have entered into such contracts with Defendant.

161. As a result of Data Breach, Plaintiffs and Class Members suffered actual damages resulting from the theft of their PII, as well as the loss of control of their PII, and remain at present risk of suffering additional damages.

162. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

163. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

FIFTH CLAIM FOR RELIEF
Invasion of Privacy
(By Plaintiffs Individually and on Behalf of the Class)

164. Plaintiffs hereby re-allege and incorporate by reference all of the allegations in paragraphs 1 to 98.

165. Plaintiffs and Class Members have a legally protected privacy interest in their PII, which is and was collected, stored, and maintained by Defendant, and they are entitled to the reasonable and adequate protection of their PII against foreseeable unauthorized access and publication of their PII to criminal actors, as occurred with the Data Breach. The PII of Plaintiffs and Class Members contain intimate details of a highly personal nature, individually and in the aggregate.

166. Plaintiffs and Class Members reasonably expected that Defendant would protect and secure their PII from unauthorized parties and that their PII would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

167. Defendant intentionally intruded into Plaintiffs' and Class Members' seclusion by disclosing without permission their PII to a third party.

168. By failing to keep Plaintiff's and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Defendant unlawfully invaded Plaintiffs' and Class Members' privacy right to seclusion by, inter alia:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. invading their privacy by improperly using their PII obtained for a specific purpose for another purpose, or disclosing it to unauthorized persons;

c. failing to adequately secure their PII from disclosure to unauthorized persons; and

d. enabling the disclosure of their PII without consent.

169. This invasion of privacy resulted from Defendant's intentional failure to properly secure and maintain Plaintiffs' and Class Members' PII, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded data.

170. Plaintiffs and Class Members' PII is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiffs', and Class Members' PII, and such information is otherwise protected from exposure to the public by various statutes, regulations and other laws.

171. The disclosure of Plaintiffs' and Class Members' PII to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

172. Defendant's willful and reckless conduct that permitted unauthorized access, exfiltration and disclosure of Plaintiffs' and Class Members' intimate and sensitive PII is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

173. The unauthorized access, exfiltration, and disclosure of Plaintiffs' and Class Members' PII was without their consent, and in violation of various statutes, regulations and other laws.

174. As a direct and proximate result of Defendant's intrusion upon seclusion, Plaintiffs and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiffs and Class Members alternatively seek an award of nominal damages.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class members, request judgment against the Defendant and the following:

A. An Order certifying the Class as defined herein, and appointing Plaintiffs and their counsel to represent the Class;

B. Equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class members' PII;

C. Injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class members, including but not limited to an order:

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

   ii. requiring Defendant to protect, including through encryption, all data

collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiffs and Class members' personal identifying information;

iv. prohibiting Defendant from maintaining Plaintiffs' and Class members' personal identifying information on a cloud-based database (if, in fact, it does so);

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

vi. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

vii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

viii. requiring Defendant to segment data by, among other things, 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;

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

x. 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 personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class members;

xi. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xii. 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;

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

xiv. requiring Defendant to meaningfully educate all Class members about the

threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xv. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvi. for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

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

E. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. Pre- and postjudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

JURY DEMAND

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

DATED: September 12, 2022

Respectfully Submitted,

By: /s/ *Carl V. Malmstrom*
Carl V. Malmstrom
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
111 W. Jackson Blvd., Suite 1700
Chicago, Illinois 60604
Tel: (312) 984-0000
Fax: (212) 686-0114
malmstrom@whafh.com

Rachele R. Byrd
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, California 92101
Tel: (619) 239-4599
Fax: (619) 234-4599
byrd@whafh.com

Attorneys for Plaintiffs