

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF CONNECTICUT**

JULIE MASON, on behalf of herself and all
others similarly situated,

Plaintiff,

v.

YALE UNIVERSITY,

Defendant.

Civil Action No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Julie Mason (“Plaintiff”), on behalf of herself and all others similarly situated, on personal knowledge as to the facts concerning herself, and on information and belief as to all other matters, and based on the investigation of counsel and public statements, brings this class action against Yale University (“Yale”).

NATURE OF THE ACTION

1. On July 26 and 27, 2018, Yale mailed letters informing individuals that, approximately one decade ago, their personal information, including names, Social Security numbers, and, in nearly all cases, dates of birth, had been accessed and extracted during a breach of its databases. In many cases, e-mail addresses and, in some cases, physical addresses were also extracted.¹ Yale discovered this data breach in June 2018 – one decade too late for any of the victims to do anything to protect themselves from the violation of their private, personal information.

¹ A copy of the letter Yale mailed can be accessed at [https://cybersecurity.yale.edu/sites/default/files/files/YALE_US_MODEL_NOTICE_2008-2009_Incident%20\(07_27_2018\).pdf](https://cybersecurity.yale.edu/sites/default/files/files/YALE_US_MODEL_NOTICE_2008-2009_Incident%20(07_27_2018).pdf) (last visited July 31, 2018)

2. According to Yale, the data breach occurred between April 2008 and January 2009, and affected approximately 119,000 individuals.²

3. The data breach affected individuals across the United States.

4. Yale admits that the data that was accessed and extracted “included names, Social Security numbers, and, in nearly all cases, dates of birth. In many cases, there was also Yale e-mail addresses and, in some cases, physical addresses.”³

5. As of August 1, 2018, Yale still has not notified all of the individuals affected by the data breach.⁴

6. None of the individuals whose personal identifying information (“PII” or “Personal Information”) was accessed authorized such access or extraction.

7. Yale itself classifies the data that was accessed, including Social Security numbers, as “High Risk,” in that it “could be exploited for criminal or other wrongful purposes.”⁵

8. Yale also admits that it is obligated by statute, regulation, and contract to keep these data confidential.⁶

9. While Yale states that the breach impacted “members of the Yale community, including alumni/ae, faculty members, and staff members,”⁷ the breach impacted a far broader range of people, as evidenced by the fact that Plaintiff’s information was accessed and extracted, despite that Plaintiff is not and never was an alumnus, faculty member, or staff member of Yale.

See infra ¶ 22.

² <https://cybersecurity.yale.edu/data-intrusion-response> (last visited July 31, 2018).

³ *Id.*

⁴ *Id.*

⁵ <https://your.yale.edu/policies-procedures/policies/1604-data-classification-policy> (last visited July 31, 2018)

⁶ *Id.*

⁷ <https://cybersecurity.yale.edu/data-intrusion-response> (last visited July 31, 2018).

10. Yale admits it knew of the unauthorized access – and thus the defect in its data security system – at least as early as June 16, 2018. Yet, despite the breadth and severity of the PII disclosures, Yale did not issue any public statement until July 26 and 27, more than a month after—and approximately 10 years after the breach occurred.

11. Yale unnecessarily kept and electronically stored in its databases “unneeded personal information” of its applicants, alums, faculty and staff, including their Social Security numbers, names, dates of birth, and addresses.

12. Yale concealed that it was keeping and storing this unneeded information from Plaintiff and the Class members.

13. Beginning in 2011, Yale states that it “deleted the personal information in [its] database as part of an effort to eliminate unneeded personal information on Yale servers.” (underlining added).⁸

14. Yale stored “unneeded personal information” on its servers, including Plaintiff’s and Class members’ Social Security numbers. In Plaintiff’s case, Yale stored this “unneeded personal information,” for over 10 years despite that Plaintiff never enrolled at Yale University. *See infra* ¶ 22.

15. Yale’s letter also states that “Yale considers the protection of personal data of the utmost importance and is taking measures to help you guard against identity theft by offering you identity monitoring services.”⁹ However, in the case of Plaintiff and other Class members, Yale’s offer is simply too little, too late.

⁸ *Id.*

⁹ [https://cybersecurity.yale.edu/sites/default/files/files/YALE_US_MODEL_NOTICE_2008-2009_Incident%20\(07_27_2018\).pdf](https://cybersecurity.yale.edu/sites/default/files/files/YALE_US_MODEL_NOTICE_2008-2009_Incident%20(07_27_2018).pdf) (last visited July 31, 2018)

16. To make matters worse, Yale's databases were breached a second time between March 2016 and June 2018.¹⁰ During that breach 33 individuals had their Personal Information, including names and Social Security numbers accessed. Again, Yale failed to discover that breach until years later.

17. Yale's actions and omissions violate well established legal and statutory duties it owed to Plaintiff and all other similarly situated persons.

18. Plaintiff brings this class action on behalf of herself and all others similarly situated for actual and statutory damages, as well as punitive damages and equitable relief to fully redress the widespread harm Yale's wrongful acts and omissions have unleashed.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this civil action pursuant to 28 U.S.C. § 1332(d) because there are more than 100 class members and the aggregate amount in controversy exceeds \$5,000,000, exclusive of interest, fees, and costs, and at least one Class member is a citizen of a state different from Yale. This Court has supplemental jurisdiction over state law claims pursuant to 28 U.S.C. § 1367.

20. This Court has personal jurisdiction over Yale because Yale's principal place of business is in New Haven, Connecticut.

21. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Yale does substantial business in this District, a substantial part of the events giving rise to Plaintiff's claims took place within this judicial District, and Yale's principal place of business is in this District.

¹⁰ <https://www.zdnet.com/article/yale-discloses-old-school-data-breach/> (last visited August 1, 2018).

THE PARTIES

22. Plaintiff Julie Mason is a citizen of New York. On July 30, 2018, Ms. Mason received a letter from Yale informing her for the first time that her PII, including her name and Social Security number (and likely her date of birth), was stored by Yale and, according to Yale, was accessed and extracted in the 2008-09 data breach. Ms. Mason was ignorant that her PII had been extracted from Yale's databases prior to receiving that letter on July 30, in part, because Yale had concealed that it was unnecessarily keeping and electronically storing her personal information. Ms. Mason is not and never was an alumnus, faculty member, or staff member of Yale. Indeed, Ms. Mason's relationship with Yale was as an applicant to a visiting student program in or around 1996. Yale charged an application fee for the application, which Ms. Mason paid. As part of the application process, Yale promised, and Ms. Mason understood, that Yale would keep her Personal Information confidential and secured. But Yale failed to do so, and her Personal Information was accessed and extracted by unauthorized users. Furthermore, Yale concealed that it would maintain Ms. Mason's Personal Information in its databases even after her application process was concluded, and Plaintiff had understood that Yale would delete or destroy her "unneeded" personal information promptly after her application process was finished. Instead, Yale unnecessarily kept and electronically stored in its databases Plaintiff's "unneeded personal information." As a result of the data breach, Ms. Mason has suffered substantial harm. For example, in or about 2009, Ms. Mason was the victim of identity theft, which included her credit card accounts being compromised, and which necessitated her having to pay money for certified mail to send credit freeze requests to all three major credit reporting agencies. Moreover, in 2014, Ms. Mason had approximately \$60,000 stolen from one of her bank accounts. The thieves were able to steal the funds by using Ms. Mason's extracted PII to

change the password on her online banking account over the telephone. Ms. Mason also devoted hours of her time to addressing the aftermath of the data breach.

23. Yale University is a private research university in New Haven, Connecticut. Yale's endowment was approximately \$27.2 billion as of 2017.

CLASS ACTION ALLEGATIONS

24. Plaintiff brings all claims as class claims under Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure.

25. Plaintiff brings her negligence, C.G.S.A. § 36a-701b, and Connecticut Unfair Trade Practices Act, C.G.S.A §§ 42-110a, *et seq.* claims on behalf of a proposed nationwide class ("**Nationwide Class**"), defined as follows:

All natural persons residing in the United States whose PII was accessed and extracted as a result of the data breach announced by Yale on or about July 26 and 27, 2018.

26. Plaintiff also brings her claims under New York consumer and data protection statutes on behalf of a proposed statewide subclass ("**New York Subclass**"), defined as follows:

All natural persons residing in New York whose PII was compromised as a result of the data breach announced by Yale on or about July 26 and 27, 2018.

27. Plaintiff also brings her negligence claim on behalf of the New York Subclass as an alternative to the Nationwide Class.

28. The Nationwide Class and the New York Subclass are referred to, collectively, as the Classes.

29. Excluded from the Classes are: the Defendant; any of its corporate affiliates; any of its directors, officers, or employees; any persons who timely elects to be excluded from any of the Classes; any government entities; and any judge to whom this case is assigned and their immediate family and court staff.

30. Plaintiff does not know the exact number of members in the Classes, but believes that there are hundreds of thousands of members.

31. Common questions of law and fact exist as to all Class members and, as appropriate, the Subclass members. The data breach was generally applicable to all the Class members and arose from a common set of acts and omissions by Yale without regard to the nature or identity of individual class members, thereby making appropriate relief with respect to the Classes as a whole.

32. The questions of law and fact common to the Classes include:

- (a) Whether Yale owed a duty to the Class members under federal or state law to protect the PII, provide timely notice of the unauthorized access, provide timely and accurate information as to the extent of the compromised PII, and provide meaningful and fair redress;
- (b) Whether Yale breached such duty;
- (c) Whether Yale's breach provided the means for the data breach;
- (d) Whether Yale was negligent in failing to design, employment, and maintain adequate security systems and protocols;
- (e) Whether Yale's negligence provided the means for the data breach;
- (f) Whether Yale knew or reasonably should have known of the vulnerabilities in its systems that allowed for the unauthorized access;
- (g) Whether Yale owed a duty to the Class members under federal or state law to protect the PII, provide timely notice of the unauthorized access, provide timely and accurate information as to the extent of the compromised PII, and provide meaningful and fair redress;
- (h) Whether Yale breached such duty;
- (i) Whether Yale's breach provided the means for the data breach;

(j) Whether Yale was negligent in failing to design, employment, and maintain adequate security systems and protocols;

(k) Whether Yale's negligence provided the means for the data breach;

(l) The appropriate injunctive and related equitable relief for the Classes; and

(m) The appropriate class-wide measure of damages for the Classes.

33. Plaintiff's claims are typical of the claims of the Class members, and Plaintiff will fairly and adequately protect the interests of the Classes. Plaintiff and all members of the Classes are similarly affected by Yale's wrongful conduct in that their PII has been exposed to criminal third parties without their authorization.

34. Plaintiff's claims arise out of the same common course of conduct giving rise to the claims of the other Class members.

35. Plaintiff's interests are coincident with, and not antagonistic to, those of the other Class members.

36. Plaintiff is represented by counsel competent and experienced in the prosecution of consumer protection and tort litigation.

37. The questions of law and fact common to the Class members predominate over any questions affecting only individual members, including legal and factual issues relating to liability and damages.

38. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Among other things, such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without the unnecessary duplication of evidence, effort and expense if numerous individual actions. The benefits of proceeding as a class, including providing injured persons or entities

with a method for obtaining redress for claims that might not be practicable to pursue individually, substantially outweigh any potential difficulties in managing this class action.

39. The prosecution of separate actions by individual Class members is not feasible and would create a risk of inconsistent or varying adjudications.

COUNT I
Negligence

40. Plaintiff incorporates by reference the allegations in the preceding paragraphs as if fully set forth herein.

41. Plaintiff brings Count I on behalf of herself, the Nationwide Class, and the New York Subclass.

42. Yale owed Plaintiff and the Class members a duty of care commensurate with the sensitive nature of the PII with which it was entrusted (particularly when aggregated and digitized). Yale created this duty through its voluntary actions in collecting and storing the PII for its own benefit, as well as by its assurances (in its Privacy Policy and elsewhere) that it would safeguard that information. In addition, given the nature of the information at issue and the means by which Yale acquires it, the relationship between Plaintiff and Class members and Yale is sufficiently close and akin to privity to give rise to a duty to them. Indeed, Yale charged – and Plaintiff paid – application fees.

43. Yale's duty required it, among other things, to design and employ cybersecurity systems, anti-hacking technologies, and intrusion detection and reporting systems sufficient to protect the PII from unauthorized access and to promptly alert Yale to any such access and enable it to determine the extent of any compromised PII.

44. Had Yale designed, employed, and maintained appropriate technological and other systems, the PII would not have been compromised or, at a minimum, Yale would have

known of the unauthorized access sooner and would be able to accurately inform Plaintiff and the other members of the Classes of the extent to which their PII has been compromised.

45. Yale breached its duties of care by, among other things, failing to maintain appropriate technological and other systems to prevent unauthorized access, to minimize the PII that any intrusion could compromise (i.e., less aggregation and weeding out unnecessary and stale data), and to promptly notify Yale of a breach and enable Yale to determine the extent of the PII that had been compromised so that, among other things, Yale could timely notice affected consumers with accurate information to begin minimizing the impact of the incident.

46. Yale's breach of its duties provided the means for third parties to access, obtain, and misuse the PII of Plaintiff and the members of the Classes without authorization. It was reasonably foreseeable that such breaches would expose the PII to criminals and other unauthorized access.

47. Yale's breach of its duties has directly and proximately injured Plaintiff and members of the Classes, including by foreseeably causing them to expend time and resources investigating the extent to which their PII has been compromised, taking reasonable steps to minimize the extent to which the breach puts their credit, reputation, and finances at risk, and taking reasonable steps (nor or in the future) to redress fraud, identity theft, and similarly foreseeable consequences of unauthorized and criminal access to their PII.

48. Plaintiff and the members of the Classes are entitled to damages in an amount to be proven at trial, and to equitable relief, including injunctive relief.

COUNT II
Breach of Security Regarding Computerized Data, C.G.S.A § 36a-701b

49. Plaintiff incorporates by reference the allegations in the preceding paragraphs as

if fully set forth herein.

50. Plaintiff brings Count II on behalf of herself and the Nationwide Class.

51. Yale is a business located in Connecticut that conducts business in Connecticut and owns, licenses, and maintains computerized data that includes personal information as covered by C.G.S.A. § 36a-701b(b). Yale also maintains computerized data that includes personal information that it does not own as covered by C.G.S.A. § 36a-701b(c).

52. Plaintiff and the Nationwide Class members' PII (e.g., Social Security numbers) includes Personal Information as covered by C.G.S.A. § 36a-701b(a).

53. Yale is required to accurately notify Plaintiff and Nationwide Class members if it becomes aware of a breach of its data security system in the most expedient time possible and without unreasonable delay, not to exceed ninety days after discovery of the breach under C.G.S.A. § 36a-701b(b).

54. Yale is required to immediately notify Plaintiff and Nationwide Class members if it becomes aware of a breach of its data security system which may have compromised personal information Yale stores but Plaintiff and Nationwide Class members own under C.G.S.A. § 36a-701b(c).

55. Because Yale was aware of a breach of its security system, it had an obligation to disclose the data breach in a timely and accurate fashion as mandated by C.G.S.A. §§ 36a-701b(b) and (c).

56. By failing to disclose the Yale data breach in an accurate and timely manner, Yale failed to comply with C.G.S.A. §§ 36a-701(b) and (c). Pursuant to C.G.S.A. § 36a-701b(g), Yale's failure to comply was an unfair trade practice under the Connecticut Unfair Trade Practices Act, C.G.S.A. §§ 42-110a, *et seq.*

57. As a direct and proximate result of Yale's violations of C.G.S.A. §§ 36a-701b(b) and (c), Plaintiff and Nationwide Class members suffered damages, as described above.

58. Plaintiff and Nationwide Class members seek relief under C.G.S.A. § 42-110g for the harm they suffered because of Yale's violations of C.G.S.A. §§ 36a-701b(b) and (c), including actual damages and equitable relief, including injunctive relief.

COUNT III

Information Security Breach and Notification Act, N.Y. Gen. Bus. Law § 899-aa

59. Plaintiff incorporates by reference the allegations in the preceding paragraphs as if fully set forth herein.

60. Plaintiff brings Count III on behalf of herself and the New York Subclass.

61. Yale is a business that owns or licenses computerized data that includes Personal Information as defined by N.Y. Gen. Bus. Law. § 899-aa(1)(a). Yale also maintains computerized data that includes Private Information which Yale does not own. Accordingly, it is subject to N.Y. Gen. Bus. Law §§ 899-aa(2) and (3).

62. Plaintiff and New York Subclass members' Private Information (e.g. Social Security numbers) includes Private Information covered by N.Y. Gen. Bus. Law § 899-aa(1)(b).

63. Yale is required to give immediate notice of a breach of security of a data system to owners of Personal Information which Yale does not own, including Plaintiff and New York Subclass members, pursuant to N.Y. Gen. Bus. Law § 899-aa(3).

64. Yale is required to accurately notify Plaintiff and New York Subclass members if it discovers a security breach, or receives notice of a security breach which may have compromised Personal Information which Yale owns or licenses, in the most expedient time possible and without unreasonable delay under N.Y. Gen. Bus. Law § 899-aa(2).

65. By failing to disclose the Yale data breach in a timely and accurate manner, Yale violated N.Y. Gen. Bus. Law §§ 899-aa(2) and (3).

66. As a direct and proximate result of Yale's violations of N.Y. Gen. Bus. Law §§ 899-aa(2) and (3), Plaintiff and New York Subclass members suffered damages, as described above.

67. Plaintiff and New York Subclass members seek relief under N.Y. Gen. Bus. Law § 899-aa(6)(b), including actual damages and injunctive relief.

COUNT IV

New York General Business Law, N.Y. Gen. Bus. Law § 349, *et seq.*

68. Plaintiff incorporates by reference the allegations in the preceding paragraphs as if fully set forth herein.

69. Plaintiff brings Count IV on behalf of herself and the New York Subclass.

70. Yale engaged in deceptive acts or practices in the conduct of its business, trade, and commerce or furnishing of services, in violation of N.Y. Gen. Bus. Law § 349, including:

- a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and New York Subclass members' PII, which was a direct and proximate cause of the Yale data breach;
- b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct a proximate cause of the Yale data breach;
- c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New York Subclass members' Personal Information, which was a direct and proximate cause of the Yale data breach;

- d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and New York Subclass members' Personal Information, including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New York Subclass members' Personal Information;
- f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and New York Subclass members' Personal Information; and
- g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and New York Subclass members' Personal Information.

71. Yale's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Yale's data security and ability to protect the confidentiality of consumers' Personal Information.

72. Yale acted intentionally, knowingly, and maliciously to violate New York's General Business Law, and recklessly disregard Plaintiff and New York Subclass members' rights.

73. As a direct and proximate result of Yale's deceptive and unlawful acts and practices, Plaintiff and New York Subclass members have suffered and will continue to suffer injury, ascertainable loss of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Personal Information.

74. Yale's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large, including the thousands of New Yorkers affected by the Yale data breach.

75. The above deceptive and unlawful practices and acts by Yale caused substantial injury to Plaintiff and New York Subclass members that they could not reasonably avoid.

76. Plaintiff and New York Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of \$50 (whichever is greater), treble damages, injunctive relief, and attorneys' fees and costs.

PRAYER FOR RELIEF

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

- a. An Order certifying each of the proposed Classes and appointing Plaintiff and his Counsel to represent the Classes;
- b. An Order enjoining Yale from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiff's and Classes' PII;
- c. An Order compelling Yale to employ and maintain appropriate systems and policies to protect consumer PII and to promptly detect, and timely and accurately report, any unauthorized access to that data;
- d. An award of compensatory, statutory, and punitive damages, in an amount to be determined;
- e. An award of reasonable attorneys' fees costs and litigation expenses, as allowable by law;
- f. Interest on all amounts awarded, as allowed by law; and
- g. Such other and further relief as this Court may deem just and proper.

JURY DEMAND

Plaintiff demands, for herself and each of the classes, a trial by jury, pursuant to the Federal Rules of Civil Procedure, of all issues so triable.

Dated: August 1, 2018

Respectfully submitted,

REARDON SCANLON LLP

By: /s/ James J. Reardon, Jr.
James J. Reardon, Jr.

James J. Reardon, Jr. (CT 13802)
45 South Main Street, 3rd Floor
West Hartford, CT 06107
Telephone: (860) 955-9455
Facsimile: (860) 920-5242
Email: james.reardon@reardonscanlon.com

BURSOR & FISHER, P.A.

Scott A. Bursor (*Pro Hac Vice Forthcoming*)
Philip L. Fraietta (*Pro Hac Vice Forthcoming*)
888 Seventh Avenue
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
Email: scott@bursor.com
pfraietta@bursor.com

Attorneys for Plaintiff