UNITED STATES DISTRICT COURT
FOR THE DISTRICT COURT OF NEW JERSEY
TRENTON DIVISION

HENGGAO CAI, individually and on behalf of all others similarly situated, Plaintiff, v. PRINCETON UNIVERSITY, Defendant.	Case No. CLASS ACTION COMPLAINT JURY DEMAND

Plaintiff Henggao Cai ("Plaintiff") brings this class action against Defendant Princeton University ("Defendant") for its failure to properly secure and safeguard Plaintiff's and Class Members' protected personally identifiable information ("PII" or "Private Information") stored within Defendant's information network.

INTRODUCTION

1. Princeton University is a private Ivy League research university in Princeton, New Jersey, United States. As of 2025, Princeton University has a total enrollment of approximately 9,106 undergraduate and graduate students,[1] 1,313 faculty (including full time, part time and visiting),[2] and 101,232 living alumni[3].

2. On no later than November 10, 2025, unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PII stored on Defendant's "University

[1] https://www.princeton.edu/meet-princeton/facts-figures.
[2] https://profile.princeton.edu/princeton-and-beyond
[3] *Id.*

Advancement" database, with the intent of engaging in the misuse of the PII, including marketing and selling Plaintiff's and Class Members' PII (hereinafter the "Data Breach").[4] Defendant has since launched an investigation to determine how its database was compromised and the impact on Plaintiff's and Class Members' PII.[5]

3. Defendant had numerous duties and obligations, including those based on affirmative representations to Plaintiff and Class Members, to keep their Private Information confidential, safe, secure, and protected from unauthorized disclosure or access.

4. Defendant failed to take precautions designed to keep individuals' PII secure including, but not limited to, adequately securing and encrypting and/or more securely encrypting its servers generally, and implementing adequate security policies to protect individuals' PII.

5. Defendant owed Plaintiff and Class Members a duty to take all reasonable and necessary measures to keep the Private Information collected safe and secure from unauthorized access. Defendant solicited, collected, used, and derived a benefit from the PII, yet breached its duties by failing to implement or maintain adequate security practices.

6. The PII compromised in the Data Breach contained highly confidential data, representing a gold mine for data thieves. The data stored in Defendant's University Advancement database included the following categories of PII:

- Name (including former name);
- Degrees and years earned;
- Details of the individuals' Princeton experience (e.g., residential college, student activities);

[4] https://oit.princeton.edu/cybersecurity-incident-information-and-faq
[5] *Id.*

- Contact information (e.g., address, telephone, email)
- Gender
- Date of birth;
- Employment and business details, including: positions, professional memberships and qualifications, and other notable achievements;
- Interests and group members;
- Select information about individuals' wealth;
- Family details and relationships with other Princeton University constituents;
- Events individuals have been invited to and whether or not individuals have responded or attended;
- Volunteer or giving activity;
- A history of communications with those individuals (e.g., emails sent by the University may record whether the email has been opened and whether any links have been clicked on);
- Information individuals have shared with Defendant or affiliated organizations; and
- Photographs and other media from Princeton and affiliated events.[6]

7. Combining all of that personal data in one easily accessible location creates inherent risk; if it leaks, as the University Advancement database has, it enables scammers, fraudsters, and phishers to craft especially compelling targeted attacks against, upon information and belief, over a hundred thousand people. Defendant's disregard of basic safeguards for this database in particular is thus uniquely inexcusable.

8. Armed with the PII accessed in the Data Breach, these bad actors would not only know who the affected individuals are, but also what they talk about, what they like, even what

[6] https://advancementdataprivacy.princeton.edu/

they do for a living. This information can expose them to identity theft, fraud, and social engineering scams.

9. In fact, Defendant recognizes this very risk and warned the impacted individuals to be "alert for unusual messages that purport to come from the University. No one from Princeton University should ever call, text, or email you asking for sensitive information such as Social Security numbers, passwords, or bank information."[7]

10. Plaintiff and Class Members have therefore suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their PII, the loss of the value of their PII, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

11. Plaintiff brings this class action lawsuit to address Defendant's inadequate safeguarding of Class Members' Private Information that they collected and maintained.

12. The potential for improper disclosure and theft of Plaintiff and Class Members' PII was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure the PII left it vulnerable to an attack.

13. Upon information and belief, Defendant failed to properly monitor and implement security practices with regard to the computer network and systems that housed the PII.

14. Plaintiff and Class Members are now at risk of fraud and scams through social engineering because of Defendant's negligent conduct as the PII that Defendant collected and maintained is now in the hands of data thieves and other unauthorized third parties.

[7] https://oit.princeton.edu/cybersecurity-incident-information-and-faq

15. Plaintiff seeks to remedy these harms on behalf of themself, and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

16. Accordingly, Plaintiff, on behalf of themself and the Class, asserts claims for negligence, breach of implied contract, breach of the implied covenant of good faith and fair dealing, and unjust enrichment.

17. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are thus entitled to injunctive and other equitable relief.

JURISDICTION AND VENUE

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

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

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

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

business in this Judicial District.

THE PARTIES

Plaintiff Henggao Cai

22. Plaintiff Henggao Cai is an adult individual and, at all relevant times herein, a resident and citizen of New Jersey, residing in West Windsor, New Jersey. Plaintiff is a victim of the Data Breach.

23. Plaintiff's information was stored with Defendant as a result of their dealings with Defendant.

24. As required in order to obtain services from Defendant, Plaintiff provided Defendant with highly sensitive personal information who then possessed and controlled it.

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

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

27. Plaintiff received an email from Defendant, dated November 15, 2025, stating that their PII was involved in the Data Breach (the "Notice").

28. Plaintiff was unaware of the Data Breach until receiving that email.

29. Plaintiff was also injured by the material risk to future harm they suffer based on Defendant's breach; this risk is imminent and substantial because Plaintiff's data has been exposed in the breach, the data involved is highly sensitive and presents a high risk of identity theft or fraud; and it is likely, given who the impacted individuals are, that some of the Class's information that has been exposed has already been misused.

30. Plaintiff suffered actual injury in the form of damages to and diminution in the value of their PII, a condition of intangible property that they entrusted to Defendant, which was

compromised in and as a result of the Data Breach.

31. Plaintiff, as a result of the Data Breach, has increased anxiety for their loss of privacy and anxiety over the impact of cybercriminals accessing, using, and selling their PII.

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

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

Defendant Princeton University

34. Defendant Princeton University is a private Ivy League research university headquartered at Princeton, NJ 08544.

FACTUAL ALLEGATIONS

A. The Data Breach

35. On no later than November 10, 2025, unauthorized third-party cybercriminals gained access to Plaintiff's and Class Members' PII stored on Defendant's "University Advancement" database, with the intent of engaging in the misuse of the PII, including marketing and selling Plaintiff's and Class Members' PII.

36. Defendant's University Advancement program acquired, collected, and stored Plaintiff's and Class Members' PII for the purpose of "for engaging alumni, parents and friends of the University to raise critically important philanthropic support for the University's highest priorities."

37. The University Advancement program "works to inform, involve, and inspire

Princeton's global community of alumni, parents and friends in ways that enable the University to fulfill its mission of advancing learning through scholarship, research and teaching to serve the nation and the world."[8]

38. The University Advancement program "is responsible for engaging alumni, parents and friends of the University to raise critically important philanthropic support for the University's highest priorities, including Annual Giving and gifts designated for a specific purpose or through estate planning. In addition, the office is responsible for ensuring that donors are both appropriately recognized and informed about the impact their gifts make on Princeton's mission of teaching and research."[9]

39. Defendant's University Program acquired, collected, and stored Plaintiff's and Class Members' PII for the purpose of alumni engagement, donor development, and other institutional advancement activities.

40. Defendant collected this information from various sources, including: directly from alumni, donors, faculty, students, parents, and other members of the University community; and from "third-party sources" such as "affiliated and related University organizations; media; public records; directories; social networks; and market research sources."[10]

41. Defendant's University Advancement program stores and maintains the following categories of PII:

- Name (including former name);
- Degrees and years earned;
- Details of the individuals' Princeton experience (e.g., residential college, student activities);

[8] https://alumni.princeton.edu/about-university-advancement
[9] *Id.*
[10] https://advancementdataprivacy.princeton.edu/

- Contact information (e.g., address, telephone, email)
- Gender
- Date of birth;
- Employment and business details, including: positions, professional memberships and qualifications, and other notable achievements;
- Interests and group members;
- Select information about individuals' wealth;
- Family details and relationships with other Princeton University constituents;
- Events individuals have been invited to and whether or not individuals have responded or attended;
- Volunteer or giving activity;
- A history of communications with those individuals (e.g., emails sent by the University may record whether the email has been opened and whether any links have been clicked on);
- Information individuals have shared with Defendant or affiliated organizations; and
- Photographs and other media from Princeton and affiliated events.[11]

42. Defendant holds such personal data and uses it "to verify an account and provide a personalized online experience; to process a gift; to support your volunteer activities; [and] to support University initiatives through philanthropic efforts."[12]

43. At all relevant times, Defendant knew or should have known, that Plaintiff and Class Members would use Defendant's services to store and/or share sensitive data, including highly confidential PII.

[11] https://advancementdataprivacy.princeton.edu/
[12] https://advancementdataprivacy.princeton.edu/

44. In Defendant's Advancement Data Privacy Policy, Defendant makes various promises to Plaintiff and Class Members about the protection of their data.

45. Defend committed to "respect[ing] and protect[ing] the privacy of alumni, donors' and affiliates' personal data."[13]

46. Defendant promised Plaintiff and Class Members that their data would be "held securely within the University," that "[a]ccess is limited on a need-to-know basis," and that "staff receive training on data protection, including compliance and confidentiality."[14]

47. Defendant also states in its Privacy Policy that it may retain this PII "in perpetuity or until the individual asks [Defendant] to remove it from [Defendant's] records."[15]

48. On November 15, 2025, Defendant announced to Plaintiff and Class Members online and via email that its University Advancement database had been compromised by third-party cyber criminals on November 10, 2025, following a "phone-phishing incident."[16] Defendant claims that the Data Breach impacted the PII of:

- All University alumni (including anyone ever enrolled as a student at Princeton even if they did not graduate)
- Alumni spouses and partners
- Widows and widowers of alumni
- Any donor to the University
- Parents of students (current and past)
- Current students

[13] https://advancementdataprivacy.princeton.edu/
[14] https://advancementdataprivacy.princeton.edu/
[15] *Id.*
[16] https://oit.princeton.edu/cybersecurity-incident-information-and-faq

- Faculty and staff (current and past)[17]

49. While the total number of individuals who have had their data exposed due to Defendant's failure to implement appropriate security safeguards is unknown at this time, it is estimated to be at least one hundred thousand based on the number of Defendant's alumni, donors, faculty, student, parents, and other members of the University community.

50. Defendant claims its investigation into the Data Breah is "ongoing" and "do[es] not at this point know precisely what information was viewed or extracted," but that the impacted "database in general contains biographical information pertaining to University fundraising and alumni engagement activities."[18]

B. The Data that Defendant Allowed to be Exfiltrated is Highly Personal and Valuable and can be Used in Harmful Ways

51. Defendant's University Advancement program is integral "to rais[ing] critically important philanthropic support for the University's highest priorities."

52. Donations from alumni, student parents, and others "is an indispensable source of revenue for [higher education] institutions" like Princeton and "critical to the[ir] financial health."[19] Because higher educational institutions regard contributions as vital, they engage in detailed capture of potential donators employment, business affiliations, volunteer history, philanthropic activity, interests, and contact information in order to identify and cultivate potential donors and to sustain participation rates.[20]

53. Data collection is likewise aimed at identifying individuals who have both

[17] https://oit.princeton.edu/cybersecurity-incident-information-and-faq
[18] https://oit.princeton.edu/cybersecurity-incident-information-and-faq
[19] https://www.hanoverresearch.com/insights-blog/higher-education/alumni-giving-university-fundraising-5-trends/
[20] https://topnonprofits.com/how-to-harness-alumni-donor-data-for-maximum-impact/

capacity and propensity to give. Studies confirm that higher education institutions conduct "predictive modeling" of likely donors and build datasets about employment, income, giving history, professional networks and volunteer activity to target them.[21] The data enables segmentation of likely donors into major-gift prospects, recurring annual donors, planned giving prospects, and volunteer-leader; thereby allowing the higher education institution to deploy its resources efficiently and maximize fundraising returns.[22]

54. In addition to identifying potential donors, higher educational institutions, like Defendant, use donor data to personalize communications, tailor events, track engagement, and deepen donor affinity and loyalty. According to Hanover Research, effective alumni giving strategies require understanding what "drives them to give and how to reach them."[23] By tracking alumni involvement, the higher educational institution uses data to structure its fundraising operations around ongoing relationship-management rather than one-time appeals.[24]

55. Finally, the number of donators and amount of contributions influence institutional rankings, future student recruitment, and donor perceptions.[25]

56. Because Defendant relies heavily on philanthropy to support its "highest priorities,"[26] its donor database contains information integral to its revenue generation, long-term planning, and strategic institutional interests. Defendant therefore derives significant operational,

---

[21] https://ir.library.illinoisstate.edu/cgi/viewcontent.cgi?article=1284&context=etd&utm; https://www.researchgate.net/publication/350865890_Fundraising_for_universities_by_alumni_efforts_a_literature_review

[22] https://www.almabase.com/blog/how-to-segment-your-alumni-audience-for-better-fundraising-outcomes

[23] https://www.hanoverresearch.com/insights-blog/higher-education/alumni-giving-university-fundraising-5-trends/

[24] *Id.*

[25] https://www.advancementform.com/resources/the-impact-of-alumni-giving-on-institutional-rankings-and-reputation

[26] https://alumni.princeton.edu/about-university-advancement

financial, and reputational benefit from the collection, retention, and use of donor information, making such data not only sensitive but intrinsically valuable to the University.

57. Personal information, like the PII Defendant collected from Plaintiff and Class Members and stored and maintained in its University Advancement database, is a valuable property right.[27]

58. Indeed, an entire economy exists related to the value of personal data. In 2023, the big data technology market was valued at roughly $349 billion, and that value is expected to grow to $397 billion by 2024.[28]

59. Because personal data is valuable personal property, market exchanges now exist where internet users like Plaintiff and Class Members can sell or monetize their own personal data. For example, in a study authored by Tim Morey, researchers studied the value that 180 internet users placed on keeping personal data secure. Contact information was valued by the study participants at approximately $4.20 per year. Demographic information was valued at approximately $3.00 per year.

60. The value of user-correlated internet data can be quantified, because companies are willing to pay users for the exact type of information.

61. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to legitimate marketers or app developers.[29] For example, consumers who agree to

[27] *See*, *e.g.*, John T. Soma, *et al*, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).
[28] https://www.fortunebusinessinsights.com/industry-reports/big-data-technology-market-100144
[29] *See*, *e.g.*, Datacoup, *The Personal Data Revolution*, https://datacoup.com/

provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[30]

62. Defendant knew or should have known the PII it collected is highly valuable to criminals. Indeed, PII is a valuable commodity for which a "cyber black market" exists in which criminals openly post phone numbers, email addresses, and other personal information on several underground internet websites.[31]

63. 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 other sources report that criminals can also purchase access to entire company data breaches from $999 to $4,995.[32]

64. Naturally, when consumer data contains greater detail about an individual, the data's value increases. Indeed, using personal data to arrange for a more personalized experience for consumers is one of the most popular and effective methods of advertising, and anyone who can provide such data to companies can earn a significant profit.

65. Given the detailed nature of the information contained in Defendant's University Advancement database, Plaintiff's and Class Members' PII is a very valuable commodity to not only Princeton, but also to third party marketers, as evidenced by the numerous companies that purchase PII from consumers.

66. Accordingly, as a result of the Data Breach, Plaintiff and Class Members lost the sale value of their PII and the opportunity to control how it is used. That a third-party data thief specifically targeted Defendant's University Advancement database demonstrates just how

[30] Nielsen Computer & Mobile Panel, Frequently Asked Questions, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html

[31] https://www.techrepublic.com/article/how-much-is-your-info-worth-on-the-darkweb-for-americans-its-just-8/

[32] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.

valuable Plaintiff's and Class Members' PII can be to data thieves and other cybercriminals.

67. While higher educational institutions, like Princeton, utilize this PII to target potential donors, cybercriminals use PII nefariously, to target victims for identity theft or other financial fraud.

68. There is a robust market on the Dark Web for illegally stolen data and the value to criminals of the PII exfiltrated here guarantees the data will be lucrative for cybercriminals to sell and re-sell on the Dark Web for years.

69. Combining all of that personal data in one easily accessible location creates inherent risk; if it leaks, as the Defendant's University Advancement database has, it enables scammers, fraudsters, and phishers to craft especially compelling targeted attacks against thousands of people. Defendant's disregard of basic safeguards for this database in particular is thus uniquely inexcusable.

70. Perhaps even more worrisome than the raw data exposed in Defendant's University Advancement database is the mapping of social identities to email addresses and other personal data.

71. Armed with the information in Defendant's University Advancement database, one would not only know who the affected individuals are, but also what they talk about, what they like, even what they do for a living. This information can be used not only to target users with ads, but also it can expose them to identity theft, fraud, and social engineering scams.

72. Here, the PII stolen from the Defendant's University Advancement database can easily be used to facilitate fraud through online scams or social engineering schemes. Social engineering is the term used for various techniques, like spear phishing and phishing,[33] used by

[33] General "phishing" typically relies on shotgun methods and mass emails to random individuals, whereas "spear phishing" focuses on specific targets based on information known about them. *See*

threat actors that are aimed at convincing a target to reveal specific information or perform specific actions.[34]

73. In a spear phishing attack, cybercriminal may leverage data about an individual to create a sophisticated, fraudulent communication to the individual (e.g., a fake email or text from "Princeton" or a phone provider requesting account payments and supplying a link for payment) that can prompt an individual to provide banking or credit card information to the criminals.

74. Phishing is another social engineering technique directed widely to groups of individuals and the most common cybercrime. The more information the cybercriminals have, the more sophisticated their phishing scams.[35]

75. Defendant specifically warned individuals impacted by the Data Breach to be "alert for unusual messages that purport to come from the University. No one from Princeton University should ever call, text, or email you asking for sensitive information such as Social Security numbers, passwords, or bank information."[36] Thus, Defendant knows or should have known Plaintiff's and Class Members' PII that it solicited, collected, used, and derived a benefit from is highly valuable to cybercriminals for social engineering purposes.

76. In 2024, New Jersey had 55,969 fraud reports from consumers and lost a total of $314,439,857 to fraud, with a median loss of $500.[37]

77. Despite this, Defendant implemented inadequate cybersecurity controls and

---

Trend Micro, *Spear phishing*, available at https://www.trendmicro.com/vinfo/us/security/definition/spear-phishing.

[34] European Union Agency for Cybersecurity, *What is Social Engineering*, available at https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering.

[35] Main, Kelly, *Phishing Statistics By State In 2024*, Forbes Advisor (June 9, 2023), available at https://www.forbes.com/advisor/business/phishing-statistics/.

[36] https://oit.princeton.edu/cybersecurity-incident-information-and-faq

[37] https://wrnjradio.com/new-jersey-consumers-reported-losing-314m-to-scams-in-2024/

measures and failed to protect Plaintiff's and Class Members' PII.

78. As a result of the Data Breach, Plaintiff's and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the PII is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

79. The fraudulent activity resulting from the Data Breach may not come to light for years.

80. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

81. Defendant is, or should have been, fully aware of the unique type and the significant volume of data on Defendant's database, amounting to thousands of individuals detailed PII and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

C. Defendant Knew or Should Have Known of the Risk of a Data Security Incident Because Higher Education Entities in Possession of Private Information Are Particularly Suspectable

82. The higher-education sector has become a recognized target for cyber-attacks, due to the quantity and sensitivity of data held by universities and their historically under-

resourced cybersecurity infrastructure.[38]

83. According to an article from DeepStrike, educational institutions experienced an average of approximately 4,388 cyberattacks per organization per week in Q2 2025 — a year-over-year increase of about 31%.[39] These attacks overwhelmingly involved credential theft, phishing, ransomware, and exploitation of unpatched or poorly configured systems.[40]

84. DeepStrike also found that this trend in cyberattacks on educational institutions is "not just increasing; it's accelerating," noting that in the first quarter of 2025 education was already the hardest-hit sector, with a 73% year-over-year increase in weekly attacks, followed by a 31% year-over-year increase in the second quarter and a continued 24% year-over-year increase in July 2025.

85. This accelerating pattern put Defendant on notice that the risk of cyberattacks against universities was both severe and worsening at the time of the breach.

86. Cyberattacks against educational institutions are a strategic choice by data thieves because educational institutions are viewed as "target rich, cyber poor" since they possess large volumes of valuable personal data while lacking robust security controls.[41]

87. Data thieves have targeted prominent American universities this year, putting Defendant on notice that adequate data protective measures were needed to protect the valuable PII of Plaintiff and Class Members in the University Advancement database.

88. On June 24, 2025, Columbia University publicly acknowledged a serious cybersecurity incident in which an unauthorized party gained network access, disrupted

[38] Mohammad Khalil, *Data Breaches in Education 2025: Why Schools Are the #1 Cyber Target*, https://deepstrike.io/blog/data-breaches-education-2025 (Aug. 18, 2025) (last accessed Nov. 17, 2025).
[39] *Id.*
[40] *Id.*
[41] *Id.*

University IT systems and "stole data from [its] network."[42] In a subsequent update dated August 5, 2025, Columbia reported that the breach included data about students, applicants and employees, including Social Security numbers, academic, financial-aid and insurance-related information.[43]

89. On or about October 31, 2025, The University of Pennsylvania ("Penn") discovered that a select group of information systems associated with its development and alumni-relations operations had been breached via a sophisticated social-engineering attack that resulted in compromised credentials.[44] Media reports suggest the possibility of up to 1.2 million alumni, donors, students or affiliates' records being involved (though Penn disputes that number).[45]

90. Defendant knew, or should have known, of this escalating threat landscape. The DeepStrike report makes clear that educational institutions faced a rapidly worsening risk profile in 2025, with cyberattack frequency and severity accelerating each quarter. By the time of Defendant's November 10, 2025 Data Breach, the vulnerabilities facing higher-education institutions were well-documented, foreseeable, and demanded Defendant implement adequate data protection methods.

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

91. Plaintiff and Class Members surrendered their highly sensitive personal data to Defendant under the implied condition that Defendant would keep it private and secure. Accordingly, Defendant also has an implied duty to safeguard their data, independent of any

[42] https://www.cuit.columbia.edu/cyber-incident
[43] https://www.cuit.columbia.edu/content/updating-our-community-cyber-incident
[44] https://university-communications.upenn.edu/data-incident
[45] *Id.*

statute.

92. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

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

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

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

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

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

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

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

100. Defendant owed a duty to Plaintiff and Class Members to encrypt and/or more reliably encrypt Plaintiff's and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

CLASS ACTION ALLEGATIONS

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

> All individuals within the United States of America whose PII was exposed to unauthorized third parties as a result of the data breach experienced by Defendant on November 10, 2025.

102. Members of the proposed Class are readily ascertainable because the class definitions are based on objective criteria

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

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

105. This action has been brought and may properly be maintained as a class action under Federal Rule of Civil Procedure Rule 23 because there is a well-defined community of

interest in the litigation, and membership in the proposed classes is easily ascertainable.

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

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

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

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

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

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

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

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

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

h. Whether Defendant's conduct, including its failure to act, resulted in or

was the proximate cause of the breach of its systems, resulting in the loss of the PII of Plaintiff and Class Members;

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

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

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

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

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

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

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

111. Superiority of Class Action: Since the damages suffered by individual Class

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

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

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

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

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

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

Procedure.

CLAIMS FOR RELIEF

COUNT ONE
Negligence
(On behalf of the Class)

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

118. At all times herein relevant, Defendant owed Plaintiff and Class Members a duty of care, *inter alia*, to act with reasonable care to secure and safeguard their PII and to use reasonable methods to do so. Defendant took on this obligation upon accepting and storing the PII of Plaintiff and Class Members in its computer systems and on its networks.

119. Among these duties, Defendant was expected:

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

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

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

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

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

victims of any inadequate security practices.

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

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

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

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

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

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

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

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

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

Defendant, Plaintiff, and/or the remaining Class Members.

130. Defendant breached its general duty of care to Plaintiff and Class Members in, but not necessarily limited to, the following ways:

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

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

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

d. by failing to adequately train its employees not to store PII longer than absolutely necessary;

e. by failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class Members' PII;

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

g. by failing to encrypt Plaintiff's and Class Members' PII and monitor user behavior and activity in order to identify possible threats.

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

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

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

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

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

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

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

138. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII 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 embarrassment and identity theft; (vi) the continued risk to their PII, which may remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

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

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

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

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

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

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

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

145. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

146. As a condition of their relationship with Defendant, Plaintiff and Class Members provided and entrusted their PII to Defendant.

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

148. Plaintiff and Class Members agreed to, and did, provide their PII to Defendant, in exchange for, amongst other things, the protection of their PII.

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

150. Defendant breached its implied contracts with Plaintiff and Class Members by failing to safeguard and protect their PII.

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

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

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

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

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

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

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

PRAYER FOR RELIEF

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

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

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

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

123. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII;

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

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

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

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

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

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

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

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

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

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

i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based

upon the employees' respective responsibilities with handling PII, as well as protecting the PII of Plaintiff and Class Members;

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

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

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

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

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

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

JURY DEMAND

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

Dated: November 18, 2025

Respectfully submitted,

By: */s/ Kevin Laukaitis*

Kevin Laukaitis (NJ ID 155742022)
LAUKAITIS LAW LLC
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

Joseph D. DePalma
Catherine B. Derenze
LITE DEPALMA GREENBERG & AFANADOR, LLC
570 Broad Street, Suite 1201
Newark, NJ 07102
Tel: 973-623-3000
Fax: 973-623-0858
jdepalma@litedepalma.com
cderenze@litedepalma.com

Attorneys for Plaintiff and the Putative Class

JS 44 (Rev. 03/24)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

HENGGAO CAI, individually and on behalf of all others similarly situated.

(b) County of Residence of First Listed Plaintiff MERCER CO., NJ
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
LAUKAITIS LAW LLC, 954 Avenida Ponce De Leon, Suite 205, #10518, San Juan, PR 00907 T: 2157894462

DEFENDANTS

PRINCETON UNIVERSITY

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

INTELLECTUAL PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding | ☐ 2 Removed from State Court | ☐ 3 Remanded from Appellate Court | ☐ 4 Reinstated or Reopened | ☐ 5 Transferred from Another District *(specify)* | ☐ 6 Multidistrict Litigation - Transfer | ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332

Brief description of cause:
Data Breach - Breach of Contract

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5000000

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
November 18, 2025

SIGNATURE OF ATTORNEY OF RECORD
/s/ Kevin Laukaitis

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of New Jersey

HENGGAO CAI, individually and on behalf of all others similarly situated,

Plaintiff(s)

v.

PRINCETON UNIVERSITY

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* PRINCETON UNIVERSITY
1 Nassau Hall
Princeton, NJ 08544

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

Kevin Laukaitis
LAUKAITIS LAW LLC
954 Avenida Ponce De Leon
Suite 205, #10518
San Juan, PR 00907

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

ClassAction.org
