Exhibit A

Onondaga Supreme Court Index Number 007718/2021 *Miller, Trevor v. Syracuse University*

eFiled Documents Detail

New York State Unified Court System

UCS COURTS

WebCivil Supreme - eFiled Documents Detail

Court: **Onondaga Supreme Court**
Index Number: **007718/2021**
Case Name: **Miller, Trevor vs. Syracuse University**
Case Type: **Comm-Other**
Track: **Standard**

Document List - Click on the document name to view the document

Document #	Date Received/Filed	Document	Description	Motion #	Filing User
1	09/02/2021	SUMMONS + COMPLAINT	--none--		TODD SETH GARBER
2	09/02/2021	RJI -RE: OTHER	Commercial Class Action		TODD SETH GARBER
3	09/02/2021	ADDENDUM - COMMERCIAL DIVISION (840C)	--none--		TODD SETH GARBER

Close

SUPREME COURT STATE OF NEW YORK
COUNTY OF ONONDAGA

TREVOR MILLER, individually and on behalf of all others similarly situated,

Plaintiff

-against-

SYRACUSE UNIVERSITY,

Defendant.

Index No. _____

Summons Filed: September 2, 2021

SUMMONS

To the above-named Defendant:

You are hereby summoned and required to answer the attached complaint of the Plaintiff in this action and to serve a copy of your answer upon the attorneys for the Plaintiff at the address stated below.

If this summons was personally delivered to you in the State of New York, you must serve the answer within 20 days after such service, excluding the day of service. If this summons was not personally delivered to you in the State of New York, you must serve the answer within 30 days after service of the summons is complete, as provided by law.

If you do not serve an answer to the attached complaint within the applicable time limitation stated above, a judgment may be entered against you, by default, for the relief demanded in the complaint.

Plaintiff designates Onondaga County as the place of trial.

The basis of venue is defendant Syracuse University's address at 900, South Crouse Ave., Syracuse, NY 13244, located in the County of Onondaga.

Dated: September 2, 2021

Respectfully Submitted,

FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP

By: */s/ Todd S. Garber*

Todd S. Garber
Andrew C. White
One North Broadway, Suite 900
White Plains, New York 10601
Tel.: (914) 298-3281
tgarber@fbfglaw.com
awhite@fbfglaw.com

Seth A. Meyer
Alex J. Dravillas
KELLER LENKNER LLC
150 N. Riverside, Suite 4270
Chicago, Illinois 60606
Tel: (312) 741-5220
sam@kellerlenkner.com
ajd@kellerlenkner.com

Attorneys for Plaintiff and the Proposed Class

SUPREME COURT STATE OF NEW YORK
COUNTY OF ONONDAGA

TREVOR MILLER, individually and on behalf of all others similarly situated,

Plaintiff

-against-

SYRACUSE UNIVERSITY,

Defendant.

Index No. _____

Date: September 2, 2021

CLASS ACTION COMPLAINT

Jury Trial Demanded

Plaintiff Trevor Miller, individually and on behalf of all other similarly situated persons, by and through his attorneys, Finkelstein, Blankinship, Frei-Pearson & Garber, LLP and Keller Lenkner LLC, and for his class action complaint against Defendant Syracuse University, respectfully alleges, upon his own knowledge or, where he lacks personal knowledge, upon information and belief including the investigation of his counsel, as follows:

INTRODUCTION

1. Plaintiff Trevor Miller ("Plaintiff" or "Mr. Miller") brings this class action lawsuit on behalf of himself and all others similarly situated against Defendant Syracuse University ("Defendant") as a result of Defendant's failure to safeguard and protect the confidential information of Mr. Miller and the other members of the Class -- including Social Security Numbers and personal information that can be used to perpetrate identity theft -- in Defendant's custody, control, and care (the "Sensitive Information").

2. Plaintiff is a student at Syracuse University. As a condition of Plaintiff's attendance, Plaintiff was required to and did supply Sensitive Information to Defendant, including, but not limited, to his Social Security Number, date of birth, financial information, and other personal private data.

3. Unbeknownst to Plaintiff, Defendant did not have sufficient cyber-security procedures and policies in place to safeguard the Sensitive Information it possessed. As a result, cybercriminals were able to gain access to at least one of Defendant's employee email accounts between approximately September 24, 2020 and September 28, 2020, following a successful "phishing" attempt that Defendant's employees failed to identify or adequately safeguard against, thereby gaining access to approximately 9,800 Class Members' Sensitive Information, including Plaintiff's, stored in that email account (the "Data Breach"). Plaintiff and members of the proposed Class have suffered damages as a result of the unauthorized and preventable disclosure of their Sensitive Information.

4. After the Data Breach compromised Plaintiff's Sensitive Information, including his Social Security Number, Plaintiff learned of an unauthorized charge on his Chase Bank checking account on or about July 13, 2021, after the Data Breach occurred. Addressing this apparent fraudulent charge on his account and preventing further bank fraud required Plaintiff to suspend and cancel his debit card and to take the time to personally go to a Chase Bank branch location to have a replacement card issued. For over a week, Plaintiff did not have access to a functional debit card, as a replacement card was not issued and received until on or about July 22, 2021.

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

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

7. Plaintiff asserts causes of action sounding in common negligence, negligent hiring and training of employees, breach of fiduciary duty, breach of contract, and delay in notification

of the Data Breach, all arising from Defendant's failure to safeguard his Sensitive Information, and he brings claims for consequential damages, injunctive relief, and punitive damages.

PARTIES

8. Plaintiff Trevor Miller is and was a resident of Onondaga County, New York, who is and was a student at Syracuse University when the Data Breach occurred, and whose Sensitive Information was compromised in the Data Breach.

9. Defendant Syracuse University is a private university located in Syracuse, New York, in Onondaga County.

10. At all times material hereto, Syracuse University acted by and through agents, employees, and representatives, who were acting in the course and scope of their respective agency or employment and/or in the promotion of Syracuse University's business, mission, and/or affairs.

JURISDICTION AND VENUE

11. This Court has jurisdiction over all causes of action asserted herein. Defendant is subject to the personal jurisdiction of this Court pursuant to CPLR 301.

12. Defendant has conducted and does conduct business in the State of New York, and is headquartered and conducts its primary operations as a university in Onondaga County, New York.

13. Venue is proper in Onondaga County pursuant to CPLR 503(a) because Plaintiff resides in Onondaga County, Defendant is located in Onondaga County, and Onondaga County is the location where a substantial part of the events or omissions giving rise to Plaintiff's claims occurred.

THE RISKS OF DATA BREACHES AND COMPROMISED SENSITIVE INFORMATION ARE WELL KNOWN

14. Defendant Syracuse University had obligations created by contract, industry standards, common law, and representations made to current, former, and prospective students to keep Plaintiff's and Class Members' Sensitive Information confidential and to protect it from unauthorized access and disclosure.

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

16. Indeed, according to a report by Risk Based Security, Inc., by the end of June, 2020 was already the "worst year on record" in terms of records exposed in data breaches.[2]

17. Therefore, Defendant clearly knew or should have known of the risks of data breaches and thus should have ensure that adequate protections were in place.

DEFENDANT ALLOWED CRIMINALS TO OBTAIN PLAINTIFF'S AND THE CLASS' SENSITIVE INFORMATION.

18. Plaintiff and Class Members were obligated to provide Defendant with their Sensitive Information as part of their relationships with Defendant.

---

[1] *See, e.g., Protecting Personal Information: A Guide for Business*, FTC, *available at* https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.

[2] *See 2020 Q3 Report*, Risk Based Security, *available at* https://pages.riskbasedsecurity.com/hubfs/Reports/2020/2020%20Q3%20Data%20Breach%20QuickView%20Report.pdf.

19. Due to inadequate security against unauthorized intrusions, including but not limited to adequate employee training to identify and avoid "phishing" attempts to gain access to email accounts, cybercriminals breached Defendant's computer systems on or about September 24, 2020. This Data Breach resulted in the criminals unlawfully obtaining access to students', alumni's, and applicants' Sensitive Information, including their identities and Social Security Numbers.

DATA BREACHES LEAD TO IDENTITY THEFT

20. Data breaches are more than just technical violations of their victims' rights. By accessing a victim's personal information, the cybercriminal can ransack the victim's life: withdraw funds from bank accounts, get new credit cards or loans in the victims' name, lock the victim out of his or her financial or social media accounts, send out fraudulent communications masquerading as the victim, file false tax returns, destroy their credit rating, and more.[3]

21. Indeed, Plaintiff Miller appears to have already been the victim of attempted bank fraud following the Data Breach, which cost him time to address and temporarily denied him access to a working debit card.

22. As the United States Government Accountability Office noted in a June 2007 report on data breaches ("GAO Report"), identity thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits, and incur charges and credit in a person's name.[4] As the GAO Report states, this type of identity theft is more harmful than any

[3] *See* https://topclassactions.com/lawsuit-settlements/privacy/data-breach/875438-recent-data-breach/ (last accessed May 7, 2019).

[4] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government

other because it often takes time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

23. In addition, the GAO Report states that victims of this type of identity theft will face "substantial costs and inconveniences repairing damage to their credit records" and their "good name."[5]

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

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

> "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[6]

26. With access to an individual's Sensitive Information, cyber criminals can do more than just empty a victim's bank account -- they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and Social Security Number to obtain government benefits; or filing a fraudulent tax return using the victim's information. In addition, identity thieves may

---

Accountability Office, *available at* <https://www.gao.gov/new.items/d07737.pdf> (last visited June 3, 2019).

[5] *Id.* at 2, 9.

[6] *Id.* at 29 (emphasis added).

obtain a job using the victim's Social Security Number, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[7]

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

DEFENDANT DELAYED NOTICE TO PLAINTIFF AND THE CLASS

28. Despite becoming aware of the Data Breach on or about September 28, 2020, Defendant only notified Plaintiff and members of the Class that its systems had been breached and that their Sensitive Information was compromised in February 2021 -- more than four months after Defendant learned that the Data Breach occurred.[8]

29. On or about February 4, 2021, Defendant sent letters to Plaintiff and other Class members advising them that their Sensitive Information had been subject to unauthorized access

[7] *See* Federal Trade Commission, *Warning Signs of Identity Theft*, *available at* https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited May 28, 2019).

[8] New York's GBL § 899-AA(2) in pertinent part provides, "Any person or business which conducts business in New York state, and which owns or licenses computerized data which includes private information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the system to any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay…". Defendant's notifications to affected individuals provided no account as to why it delayed sending such notification.

and had been compromised on or about September 24, 2020 (the "Letter Notification"). A copy of the Letter Notification that Plaintiff received is attached as Exhibit A to this Complaint. The Letter Notification offered only a single year of credit monitoring through Experian IdentityWorks, and only for individuals who signed up for such monitoring by April 4, 2021.

DEFENDANT'S OBLIGATIONS AND ITS NEGLIGENT FAILURE TO MEET THEM

30. In the ordinary course of, and as a condition of, his enrollment as a student at Syracuse University, Plaintiff, like thousands of other students, alumni, and applicants, provided Sensitive Information, including but not limited to his Social Security Number, to Defendant.

31. Defendant Syracuse University maintains this Sensitive Information within its data infrastructure, including in employees' email accounts.

32. Furthermore, Plaintiff and Class Members all entered into written agreements with Defendant as part of, and as a precondition to, application and enrollment at Syracuse University. These agreements contained or incorporated representations that Defendant would protect Class Members' Sensitive Information. The agreements involved a mutual exchange of consideration whereby Defendant provided enrollment at Syracuse University for Class Members in exchange for payment from Class Members.

33. Defendant's representations to Class Members include that it adheres to the following privacy policy (the "Privacy Policy"):

> Syracuse University is committed to ensuring that your privacy is protected. Should we ask you to provide certain information by which you can be identified when using this website or through other mechanisms, you can be assured that it will only be used in accordance with this privacy policy.
>
> [. . .]
>
> We are committed to ensuring that your information is secure. In order to prevent unauthorized access or disclosure, we have put in place suitable physical, electronic, and managerial procedures to safeguard and secure the information we collect online.

The Privacy Policy enumerates specific limited circumstances for which Defendant will disclose Sensitive Information, including for purposes of answering Class Members' questions, internal record keeping, improving Syracuse University's services, contacting Class Members via promotional emails, contacting Class Members in connection with market research, and as necessary in connection with legal proceedings or where legally required to provide such information to a court or regulator.[9]

34. None of these enumerated circumstances apply to Defendant's disclosure of Sensitive Information in the Data Breach.

35. Defendant's Privacy Policy explicitly states that outside of these enumerated circumstances: "we will treat your personal data as private and will not disclose it to third parties without your knowledge."[10]

36. By negligently failing to adequately protect Plaintiff's and Class Members' Sensitive Information, Defendant violated its legal obligations and its contractual obligations embodied in its Privacy Policy.

37. Defendant compounded the actual and potential harm arising from the Data Breach by not notifying Plaintiff and other Class Members of the compromise of their personal information until February 2021, when the Letter Notification was sent. Defendant suggested in the Letter Notification that Plaintiff and Class Members review account statements, monitor credit reports, and perhaps institute security freezes on their financial accounts to safeguard their

[9] https://www.syracuse.edu/about/site/privacy-policy/; archived version from Sept. 22, 2020 available at https://web.archive.org/web/20200922105623/https://www.syracuse.edu/about/site/privacy-policy/.

[10] *Id.*

financial well-being from harm arising from the Data Breach. Defendant's unjustified delay in notifying Plaintiff and the Class that they were victims of the Data Breach will dilute any salutary effect that might come from these suggestions.

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

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

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

c. Properly monitoring its own data security systems for existing intrusions; and

d. Ensuring that agents, employees, and others with access to Sensitive Information employed reasonable security procedures.

39. Plaintiff and all members of the Class have consequently suffered harm by virtue of the compromise and exposure of their Sensitive Information -- including, but not limited to, (i) an imminent risk of future identity theft; (ii) lost time and money expended to mitigate the threat of identity theft; (iii) diminished value of personal information; and (iv) a loss of privacy. Plaintiff and Class Members were also injured because they did not receive the full value of the services for which they bargained; to wit, educational services plus adequate data security. Plaintiff and all members of the proposed Class are and will continue to be at imminent risk for tax fraud and identify theft and the attendant dangers thereof for the rest of their lives because their Sensitive Information, including Social Security Numbers, is in the hands of cyber-criminals.

DEFENDANT'S INADEQUATE RESPONSE TO THE DATA BREACH

40. Defendant's Letter Notification stated that it had "enhance[d] the security of [its] network" by "hiring additional resources for cybersecurity training and providing additional training on cybersecurity and phishing for all of [their] employees with access to personal

information."[11] No details were provided, and thus it cannot be determined from the Letter Notification whether Defendant did any of the foregoing, or if it did, whether these enhancements are sufficient to prevent recurrences similar to the Data Breach.

41. The belated Letter Notification also included an offer from Defendant of one year of free credit monitoring and identity theft resolution services through a third party provider, Experian. Defendant, however, offered an unreasonably short window of opportunity to claim these services, with victims of the Data Breach needing to claim these services by April 4, 2021, or be closed out. In addition, one year of credit monitoring services is insufficient, given that Plaintiff's and the Class Members' risk of identity theft will continue throughout their lives.

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

CLASS ALLEGATIONS

43. This action is brought on behalf of Plaintiff and all similarly situated persons pursuant to Civil Practice Law and Rules 901, *et seq.* The Class is defined as:

> All persons whose Sensitive Information, provided to Defendant as part of their application to or enrollment at Syracuse University, was exposed to unauthorized access by way of the data breach of Defendant's computer system on or about September 24, 2020.

[11] Exhibit A.

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

45. Plaintiff is a member of the Class.

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

47. This action seeks both injunctive relief and damages.

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

49. **Numerosity of the Class.** According to contemporaneous reporting on the Data Breach, the Data Breach affected approximately 9,800 individuals.[12] Therefore, the members of the Class are so numerous that their individual joinder is impracticable. The precise number of persons in the Class and their identities and addresses may be ascertained or corroborated from Defendant's records. If deemed necessary by the Court, members of the Class may be notified of the pendency of this action.

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

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

[12]https://dailyorange.com/2021/02/names-social-security-numbers-of-syracuse-university-students-exposed-in-data-breach/

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

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

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

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

52. **Adequacy.** Plaintiff will fairly and adequately represent the Class on whose behalf this action is prosecuted. His interests do not conflict with the interests of the Class.

53. Plaintiff and his chosen attorneys -- Finkelstein, Blankinship, Frei-Pearson & Garber, LLP ("FBFG") and Keller Lenkner, LLC ("Keller Lenkner") -- are familiar with the subject matter of the lawsuit and have full knowledge of the allegations contained in this Complaint.

54. FBFG has been appointed as lead counsel in several complex class actions across the country and has secured numerous favorable judgments in favor of its clients, including in cases involving data breaches. FBFG's attorneys are competent in the relevant areas of the law and have sufficient experience to vigorously represent the Class Members. Finally, FBFG possesses the financial resources necessary to ensure that the litigation will not be hampered by a lack of financial capacity and is willing to absorb the costs of the litigation.

55. Keller Lenkner is the 2021 Trial Strategy Innovation Law Firm of the Year, as named by The National Law Journal and American Lawyer Media. Keller Lenkner is national firm that has secured recovery on behalf of hundreds of thousands of plaintiffs across America and

is dedicated to zealously representing members of the Class. Keller Lenkner has the financial resources and staffing necessary to support the costs of this litigation.

56. **Superiority.** A class action is superior to any other available method for adjudicating this controversy. The proposed class action is the surest way to fairly and expeditiously compensate such a large a number of injured persons, to keep the courts from becoming paralyzed by hundreds -- if not thousands -- of repetitive cases, and to reduce transaction costs so that the injured Class Members can obtain the most compensation possible.

57. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which in any event might cause inconsistent results.

b. When the liability of Defendant has been adjudicated, the Court will be able to determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendant to all Class Members, in terms of money damages due and in terms of equitable relief, can be determined in this single proceeding rather than in multiple, individual proceedings where there will be a risk of inconsistent and varying results.

c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class Members are forced to bring individual suits, the transactional costs, including those incurred by Defendant, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with the identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class Members and as to Defendant.

d. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only Syracuse University students, alumni, and applicants, the legal and factual issues are narrow and easily defined, and the Class membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class Members can be identified from Defendant's records, such that direct notice to the Class Members would be appropriate.

58. In addition, Defendant has acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive or equitable relief with respect to the Class.

FIRST CAUSE OF ACTION

NEGLIGENCE IN THE HANDLING OF PLAINTIFF'S AND THE CLASS' SENSITIVE INFORMATION

59. Plaintiff repeats each and every allegation of this Complaint as if fully set forth at length herein.

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

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

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

63. In addition, Defendant had a duty to use reasonable security measures under Section A of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

64. Defendant's duty to use reasonable care in protecting the Sensitive Information arose not only as a result of the common law and the statutes and regulations described above, but

also because they are bound by, and have committed to comply with, industry standards for the protection of confidential information.

65. Defendant breached its common law, statutory, and other duties -- and thus, was negligent -- by failing to use reasonable measures to protect students', alumni's, and applicants' Sensitive Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiff's and the Class Members' Sensitive Information;

b. failing to adequately monitor the security of its networks and systems;

c. allowing unauthorized access to Plaintiff's and the Class Members' Sensitive Information; and

d. failing to warn Plaintiff and other Class Members about the Data Breach in a timely manner so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

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

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

68. It was therefore foreseeable that the failure to adequately safeguard Sensitive Information would result in one or more of the following injuries to Plaintiff and the members of the proposed Class: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen

confidential data; the illegal sale of the compromised data on the deep web black market; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

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

70. As a result of the foregoing, the Defendant unlawfully breached its duty to use reasonable care to protect and secure the Sensitive Information of Plaintiff and the Class which Plaintiff and members of the Class were required to provide to Defendant as a condition of application to or enrollment at Syracuse University.

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

72. Defendant's negligence was the proximate cause of harm to Plaintiff and members of the Class.

73. Had Defendant not failed to implement and maintain adequate security measures to protect the Sensitive Information of its students, alumni, and applicants, the Plaintiff's and Class

Members' Sensitive Information would not have been exposed to unauthorized access and stolen, and they would not have suffered any harm.

74. However, as a direct and proximate result of Defendant's negligence, Plaintiff and members of the Class have been seriously and permanently damaged by the Data Breach. Specifically, Plaintiff and members of the Class have been injured by, among other things; (1) the loss of the opportunity to control how their Sensitive Information is used; (2) diminution of value and the use of their Sensitive Information; (3) compromise, publication and/or theft of the Plaintiff's and the Class Members' Sensitive Information; (4) out-of-pocket costs associated with the prevention, detection and recovery from identity theft and/or unauthorized use of financial and medical accounts; (5) lost opportunity costs associated with their efforts expended and the loss of productivity from addressing as well as attempting to mitigate the actual and future consequences of the breach including, but not limited to, efforts spent researching how to prevent, detect, and recover from identity data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased cost of the use, the use of credit, credit scores, credit reports, and assets; (7) unauthorized use of compromised Sensitive Information to open new financial and/or healthcare and/or medical accounts; (8) tax fraud and/or other unauthorized charges to financial, healthcare or medical accounts and associated lack of access to funds while proper information is confirmed and corrected and/or imminent risk of the foregoing; (9) continued risks to their Sensitive Information, which remains in the Defendant's possession and may be subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Sensitive Information in its possession; and (10) future costs in terms of time, effort and money that will be spent trying to prevent, detect, contest and repair the effects of the Sensitive Information

compromised as a result of the Data Breach as a remainder of the Plaintiff's and Class Members' lives.

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

SECOND CAUSE OF ACTION

BREACH OF EXPRESS CONTRACT

76. Plaintiff repeats each and every allegation of this Complaint as if fully set forth at length herein.

77. Plaintiff and Class Members entered into written agreements with Defendant as part of, and as a precondition to, application to and enrollment at Syracuse University. These agreements contained or incorporated representations that Defendant would protect Class Members' Sensitive Information and, on information and belief, include or incorporate Defendant's Privacy Policy. The agreements involved a mutual exchange of consideration whereby Defendant provided (or committed to considering to provide) educational services for Class Members in exchange for payment from Class Members.

78. Defendant's failure to protect Class Members' Sensitive Information constitutes a material breach of the terms of the agreement by Defendant as reflected, *inter alia*, in its Privacy Policy.

79. As a direct and proximate result of Defendant's breach of contract with Plaintiff and Class Members, Plaintiff and Class Members have been irreparably harmed.

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

THIRD CAUSE OF ACTION

BREACH OF IMPLIED CONTRACT

81. Plaintiff repeats each and every allegation of this Complaint as if fully set forth at length herein.

82. Plaintiff and members of the Class provided Sensitive Information to the Defendant in connection with their obtaining educational services from Defendant and were required to provide their Sensitive Information as a condition of receiving services therefrom.

83. Defendant would not have enrolled Plaintiff, nor any members of the Class had Plaintiff and members of the Class not provided various forms of Sensitive Information to Defendant, including their Social Security Numbers and other privileged and confidential items of information.

84. Plaintiff and members of the Class had no alternative and did not have any bargaining power with regards to providing their Sensitive Information. The Defendant required disclosure of Sensitive Information as a condition to providing its services, which the Plaintiff and members of the Class did.

85. When Plaintiff and Class Members paid money and provided their Sensitive Information to Defendant in exchange for services, they entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to timely and accurately notify them if their data had been breached and compromised.

86. Defendant solicited and invited prospective students and other consumers to provide their Sensitive Information as part of its regular business practices. These individuals accepted Defendant's offers and provided their Sensitive Information to Defendant. In entering into such implied contracts, Plaintiff and the Class reasonably assumed that Defendant's data

security practices and policies were reasonable and consistent with industry standards, and that Defendant would use part of the funds received from Plaintiff and the Class to pay for adequate and reasonable data security practices.

87. Plaintiff and the Class would not have provided and entrusted their Sensitive Information to Defendant in the absence of the implied contract between them and Defendant to keep the information secure.

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

89. Defendant breached its implied contracts with Plaintiff and the Class by failing to safeguard and protect their Sensitive Information and by failing to provide timely and accurate notice that their personal information was compromised as a result of the Data Breach.

90. As a direct and proximate result of Defendant's breaches of their implied contracts, Plaintiff and the Class sustained actual losses and damages as described herein.

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

FOURTH CAUSE OF ACTION

VIOLATION OF NEW YORK GENERAL BUSINESS LAW § 899-AA

92. Plaintiff repeats each and every allegation of this Complaint as if fully set forth at length herein.

93. Defendant "became aware" of what it called "suspicious activity related to its systems" by no later than January 4, 2021, and likely as early as September, 2020. Defendant admitted that "an unauthorized actor" -- a hacker or hackers -- had gained access to its systems and the Sensitive Information contained therein on or about September 24, 2021.

94. Despite the dates of the foregoing, the Defendant failed to provide notification to Plaintiff and members of the Class for four months, until February 2021, when the Letter Notification was sent out.

95. Pursuant to General Business Law § 899-AA(2), the Defendant was obligated to provide disclosure to the victims of a data breach within "the most expedient time possible and without unreasonable delay…"

96. The Defendant, in delaying four months to notify the Plaintiff and members of the Class of the Data Breach, violated General Business Law § 899-AA(2).

97. Plaintiff demands compensation from the Defendant for all damages that resulted from the delay in providing notification as required by law under General Business Law § 899-AA(2).

FIFTH CAUSE OF ACTION

VIOLATION OF NEW YORK GENERAL BUSINESS LAW § 349

98. Plaintiff repeats each and every allegation of this Complaint as if fully set forth at length herein.

99. Defendant, while operating in New York, engaged in deceptive acts and practices in the conduct of business, trade, and commerce and the furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a). This includes but is not limited to the following:

a. Defendant failed to enact adequate privacy and security measures to protect the Class Members' Sensitive Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach;

b. Defendant failed to take proper action following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Defendant knowingly and deceptively misrepresented that it would maintain adequate data privacy and security practices and procedures to safeguard the Sensitive Information from unauthorized disclosure, release, data breaches, and theft;

d. Defendant knowingly and deceptively misrepresented that it would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Sensitive Information; and

e. Defendant failed to disclose the Data Breach to the victims in a timely and accurate manner, in violation of the duties imposed by, *inter alia*, N.Y. Gen Bus. Law § 899-aa(2).

100. As a direct and proximate result of Defendant's practices, Plaintiff and other Class Members suffered injury and/or damages, including, but not limited to, 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 Sensitive Information.

101. The above unfair and deceptive acts and practices by Defendant were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and other Class Members that they could not reasonably avoid, which outweighed any benefits to consumers or to competition.

102. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard Sensitive Information entrusted to it, and that risk of a data breach or theft was highly likely. Defendant's actions in engaging in the above-named unfair practices and deceptive acts were negligent, knowing, and willful.

103. Plaintiff seeks relief under N.Y. Gen. Bus. Law § 349(h) for actual damages (to be proven at trial), injunctive relief, and/or attorney's fees and costs. Plaintiff does not seek statutory damages.

104. Plaintiff and Class Members seek to enjoin the unlawful deceptive acts and practices described above. Each Class Member will be irreparably harmed unless the Court enjoins Defendant's unlawful, deceptive actions, because, as detailed herein, Defendant will continue to fail to protect Sensitive Information entrusted to it.

105. Plaintiff and Class Members seek declaratory relief, restitution for monies wrongfully obtained, disgorgement of ill-gotten revenues and/or profits, injunctive relief prohibiting Defendant from continuing to disseminate its false and misleading statements, and other relief allowable under N.Y. Gen. Bus. Law § 349.

SIXTH CAUSE OF ACTION

INJUNCTION UNDER CPLR ARTICLE 63

106. Plaintiff repeats each and every allegation of this Complaint as if fully set forth at length herein.

107. The Restatement (Second) of Torts states:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 652B (1977)

108. Plaintiff and Class Members had a reasonable expectation of privacy in the Sensitive Information that Defendant mishandled. Plaintiff and Class Members maintain a privacy interest in their Sensitive Information, which is private, confidential information that is also protected from disclosure by applicable laws set forth above.

109. Plaintiff's and Class Members' Sensitive Information was contained, stored, and managed electronically in Defendant's records, computers, and databases that was intended to be secured from unauthorized access to third-parties because it contained highly sensitive, confidential matters regarding Plaintiff's and Class Members' identities, including Social Security numbers, that were only shared with Defendant for the limited purpose of obtaining Defendant's educational services.

110. Additionally, Plaintiff's and Class Members' Sensitive Information, when contained in electronic form, is highly attractive to criminals who can nefariously use their Sensitive Information for fraud, identity theft, and other crimes without their knowledge and consent.

111. Defendant unlawfully intruded upon Plaintiff's and Class Members' solitude, seclusion, or private affairs. Defendant's disclosure of Plaintiff's and Class Members' Sensitive Information to unauthorized third parties as a result of its failure to adequately secure and safeguard their Personal Information is offensive to a reasonable person.

112. Defendant's disclosure of Plaintiff's and Class Members' Sensitive Information to unauthorized third parties permitted the physical and electronic intrusion into Plaintiff's and Class Members' private quarters where their Sensitive Information was stored and disclosed private facts about them (including their Social Security numbers) into the public domain (in this case, the dark web).

113. In failing to protect Plaintiff's and Class Members' Sensitive Information, and in intentionally misusing and/or disclosing their Sensitive Information, Defendant acted with intentional malice and oppression and in conscious disregard of Plaintiff's and Class Members' rights to have such information kept confidential and private.

114. Plaintiff and Class Members have been damaged by Defendant's conduct, by incurring the harms and injuries arising from the Data Breach now and in the future. Plaintiff, therefore, seeks an award of damages on behalf of himself and the Class.

SEVENTH CAUSE OF ACTION

INJUNCTION UNDER CPLR ARTICLE 63

115. Plaintiff repeats each and every allegation of this Complaint as if fully set forth at length herein.

116. Plaintiff seeks an injunction from this Court compelling Defendant to implement cyber-security policies and procedures equal to or better than industry standards.

117. As alleged herein, the failures of the Defendant to implement adequate cyber-security measures and protocols has led to the compromise of the Sensitive Information Plaintiff and members of the Class were required to provide as a condition of obtaining educational services from Defendant, resulting in irreparable harm.

118. Defendant remains in possession of the Sensitive Information of Plaintiff and the Class. It is imperative that the Court intervene to assure that the Defendant takes all reasonable steps to protect that Sensitive Information lest there be another data breach.

119. Plaintiff and the Class have no other adequate remedy at law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Trevor Miller demands judgment on behalf of himself and the Class as follows:

a. Certifying that the action may be maintained as a class action and appointing the named Plaintiff to be class representative and the undersigned counsel to be Class counsel;

b. Requiring that Defendant pay for notifying the members of the Class of the pendency of this suit;

c. Awarding Plaintiff and the Class appropriate relief, including actual damages, compensatory damages, and punitive damages on the First, Second, Third, Fourth, Fifth, and Sixth Causes of Action;

d. Awarding injunctive relief on the Seventh Cause of Action requiring Defendant to safeguard the Sensitive Information of all persons providing Sensitive Information to the it as part of and as a condition of obtaining Defendant's services;

e. Awarding Plaintiff and the Class prejudgment and post-judgment interest;

f. Awarding Plaintiff and the Class their attorneys' fees and costs pursuant to CPLR 909 and other applicable laws, together with their costs and disbursements of this action; and

g. Awarding such other and further relief as the Court may deem just and proper.

DEMAND FOR TRIAL BY JURY

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

Dated: September 2, 2021

Respectfully Submitted,

FINKELSTEIN, BLANKINSHIP, FREI-PEARSON & GARBER, LLP

By: */s/ Todd S. Garber*

Todd S. Garber
Andrew C. White
One North Broadway, Suite 900
White Plains, New York 10601
Tel.: (914) 298-3281
tgarber@fbfglaw.com
awhite@fbfglaw.com

Seth A. Meyer
Alex J. Dravillas
KELLER LENKNER LLC
150 N. Riverside, Suite 4270
Chicago, Illinois 60606
Tel: (312) 741-5220
sam@kellerlenkner.com
ajd@kellerlenkner.com

Attorneys for Plaintiff and the Proposed Class

REQUEST FOR JUDICIAL INTERVENTION

UCS-840
(rev. 07/29/2019)

Onondaga Supreme COURT, COUNTY OF Onondaga

Index No: _____ Date Index Issued: _____

For Court Use Only:
IAS Entry Date
Judge Assigned
RJI Filed Date

CAPTION Enter the complete case caption. Do not use et al or et ano. If more space is needed, attach a caption rider sheet.

Trevor Miller

Plaintiff(s)/Petitioner(s)

-against-

Syracuse University

Defendant(s)/Respondent(s)

NATURE OF ACTION OR PROCEEDING: Check only one box and specify where indicated.

COMMERCIAL

- ☐ Business Entity (includes corporations, partnerships, LLCs, LLPs, etc.)
- ☐ Contract
- ☐ Insurance (where insurance company is a party, except arbitration)
- ☐ UCC (includes sales and negotiable instruments)
- ☒ Other Commercial (specify): Commercial Class Action

NOTE: *For Commercial Division assignment requests pursuant to 22 NYCRR 202.70(d), complete and attach the* ***COMMERCIAL DIVISION RJI ADDENDUM (UCS-840C)****.*

REAL PROPERTY: Specify how many properties the application includes: _____

- ☐ Condemnation
- ☐ Mortgage Foreclosure (specify): ☐ Residential ☐ Commercial

Property Address: _____

NOTE: *For Mortgage Foreclosure actions involving a one to four-family, owner-occupied residential property or owner-occupied condominium, complete and attach the* ***FORECLOSURE RJI ADDENDUM (UCS-840F)****.*

- ☐ Tax Certiorari - Section: Block: Lot:
- ☐ Tax Foreclosure
- ☐ Other Real Property (specify): _____

OTHER MATTERS

- ☐ Certificate of Incorporation/Dissolution [see ***NOTE*** in **COMMERCIAL** section]
- ☐ Emergency Medical Treatment
- ☐ Habeas Corpus
- ☐ Local Court Appeal
- ☐ Mechanic's Lien
- ☐ Name Change
- ☐ Pistol Permit Revocation Hearing
- ☐ Sale or Finance of Religious/Not-for-Profit Property
- ☐ Other (specify): _____

MATRIMONIAL

- ☐ Contested

NOTE: *If there are children under the age of 18, complete and attach the* ***MATRIMONIAL RJI Addendum (UCS-840M)****.*

For Uncontested Matrimonial actions, use the Uncontested Divorce RJI ***(UD-13)****.*

TORTS

- ☐ Asbestos
- ☐ Child Victims Act
- ☐ Environmental (specify): _____
- ☐ Medical, Dental, or Podiatric Malpractice
- ☐ Motor Vehicle
- ☐ Products Liability (specify): _____
- ☐ Other Negligence (specify): _____
- ☐ Other Professional Malpractice (specify): _____
- ☐ Other Tort (specify): _____

SPECIAL PROCEEDINGS

- ☐ CPLR Article 75 (Arbitration) [see ***NOTE*** in **COMMERCIAL** section]
- ☐ CPLR Article 78 (Body or Officer)
- ☐ Election Law
- ☐ Extreme Risk Protection Order
- ☐ MHL Article 9.60 (Kendra's Law)
- ☐ MHL Article 10 (Sex Offender Confinement-Initial)
- ☐ MHL Article 10 (Sex Offender Confinement-Review)
- ☐ MHL Article 81 (Guardianship)
- ☐ Other Mental Hygiene (specify): _____
- ☐ Other Special Proceeding (specify): _____

STATUS OF ACTION OR PROCEEDING: Answer YES or NO for every question and enter additional information where indicated.

	YES	NO	
Has a summons and complaint or summons with notice been filed?	☒	☐	If yes, date filed: 09/02/2021
Has a summons and complaint or summons with notice been served?	☐	☒	If yes, date served: _____
Is this action/proceeding being filed post-judgment?	☐	☒	If yes, judgment date: _____

NATURE OF JUDICIAL INTERVENTION: Check one box only and enter additional information where indicated.

- ☐ Infant's Compromise
- ☐ Extreme Risk Protection Order Application
- ☐ Note of Issue/Certificate of Readiness
- ☐ Notice of Medical, Dental, or Podiatric Malpractice — Date Issue Joined: _____
- ☐ Notice of Motion — Relief Requested: _____ Return Date: _____
- ☐ Notice of Petition — Relief Requested: _____ Return Date: _____
- ☐ Order to Show Cause — Relief Requested: _____ Return Date: _____
- ☐ Other Ex Parte Application — Relief Requested: _____
- ☐ Poor Person Application
- ☐ Request for Preliminary Conference
- ☐ Residential Mortgage Foreclosure Settlement Conference
- ☐ Writ of Habeas Corpus
- ☒ Other (specify): Commercial Class Action

RELATED CASES: List any related actions. For Matrimonial cases, list any related criminal or Family Court cases. If none, leave blank. If additional space is required, complete and attach the **RJI Addendum (UCS-840A)**.

Case Title	Index/Case Number	Court	Judge (if assigned)	Relationship to instant case

PARTIES: For parties without an attorney, check the "Un-Rep" box and enter the party's address, phone number and email in the space provided. If additional space is required, complete and attach the **RJI Addendum (UCS-840A)**.

Un-Rep	Parties List parties in same order as listed in the caption and indicate roles (e.g., plaintiff, defendant; 3rd party plaintiff, etc.)	Attorneys and/or Unrepresented Litigants For represented parties, provide attorney's name, firm name, address, phone and email. For unrepresented parties, provide party's address, phone and email.	Issue Joined For each defendant, indicate if issue has been joined.	Insurance For each defendant, indicate insurance carrier, if applicable.
☐	Name: Miller, Trevor Role(s): Plaintiff/Petitioner	TODD GARBER, Finkelstein, Blankinship, Frei-Pearson & Garber, LLP, 1 N BROADWAY STE 900 , White Plains, NY 10601, (914) 298-3283, tgarber@fbfglaw.com	☐ YES ☒ NO	
☒	Name: Syracuse University Role(s): Defendant/Respondent	900 South Crouse Ave, Syracuse, NY 13244	☐ YES ☒ NO	
☐	Name: Role(s):		☐ YES ☐ NO	
☐	Name: Role(s):		☐ YES ☐ NO	
☐	Name: Role(s):		☐ YES ☐ NO	
☐	Name: Role(s):		☐ YES ☐ NO	
☐	Name: Role(s):		☐ YES ☐ NO	
☐	Name: Role(s):		☐ YES ☐ NO	
☐	Name: Role(s):		☐ YES ☐ NO	

I AFFIRM UNDER THE PENALTY OF PERJURY THAT, UPON INFORMATION AND BELIEF, THERE ARE NO OTHER RELATED ACTIONS OR PROCEEDINGS, EXCEPT AS NOTED ABOVE, NOR HAS A REQUEST FOR JUDICIAL INTERVENTION BEEN PREVIOUSLY FILED IN THIS ACTION OR PROCEEDING.

Dated: 09/02/2021

TODD SETH GARBER
Signature

4129300
Attorney Registration Number

TODD SETH GARBER
Print Name

This form was generated by NYSCEF

Print Form

UCS-840C
3/2011

SUPREME COURT OF THE STATE OF NEW YORK

COUNTY OF _____

_____x

Trevor Miller

Plaintiff(s)/Petitioner(s)

-against-

Syracuse University

Defendant(s)/Respondent(s)

_____x

Index No. _____

RJI No. (if any) _____

COMMERCIAL DIVISION

Request for Judicial Intervention Addendum

COMPLETE WHERE APPLICABLE [add additional pages if needed]:

Plaintiff/Petitioner's cause(s) of action [check all that apply]:

- [x] Breach of contract or fiduciary duty, fraud, misrepresentation, business tort (e.g. unfair competition), or statutory and/or common law violation where the breach or violation is alleged to arise out of business dealings (e.g. sales of assets or securities; corporate restructuring; partnership, shareholder, joint venture, and other business agreements; trade secrets; restrictive covenants; and employment agreements not including claims that principally involve alleged discriminatory practices)
- [ ] Transactions governed by the Uniform Commercial Code (exclusive of those concerning individual cooperative or condominium units)
- [ ] Transactions involving commercial real property, including Yellowstone injunctions and excluding actions for the payment of rent only
- [ ] Shareholder derivative actions — without consideration of the monetary threshold
- [x] Commercial class actions — without consideration of the monetary threshold
- [ ] Business transactions involving or arising out of dealings with commercial banks and other financial institutions
- [ ] Internal affairs of business organizations
- [ ] Malpractice by accountants or actuaries, and legal malpractice arising out of representation in commercial matters
- [ ] Environmental insurance coverage
- [ ] Commercial insurance coverage (e.g. directors and officers, errors and omissions, and business interruption coverage)
- [ ] Dissolution of corporations, partnerships, limited liability companies, limited liability partnerships and joint ventures — without consideration of the monetary threshold
- [ ] Applications to stay or compel arbitration and affirm or disaffirm arbitration awards and related injunctive relief pursuant to CPLR Article 75 involving any of the foregoing enumerated commercial issues — without consideration of the monetary threshold

Plaintiff/Petitioner's claim for compensatory damages [exclusive of punitive damages, interest, costs and counsel fees claimed]:

$ _____

Plaintiff/Petitioner's claim for equitable or declaratory relief [brief description]:

Plaintiff Trevor Miller (Plaintiff or Mr. Miller) brings this class action lawsuit on behalf of himself and all others similarly situated against Defendant Syracuse University (Defendant) as a result of Defendant s failure to safeguard and protect the confidential information of Mr. Miller and the other members of the Class -- including Social Security Numbers and personal information that can be used to perpetrate identity theft -- in Defendant s custody, control, and care (the Sensitive Information).

Defendant/Respondent's counterclaim(s) [brief description, including claim for monetary relief]:

I REQUEST THAT THIS CASE BE ASSIGNED TO THE COMMERCIAL DIVISION. I CERTIFY THAT THE CASE MEETS THE JURISDICTIONAL REQUIREMENTS OF THE COMMERCIAL DIVISION SET FORTH IN 22 NYCRR § 202.70(a), (b) AND (c).

Dated: 9/2/21

/s/ Todd S. Garber
_____
SIGNATURE

Todd S. Garber
_____
PRINT OR TYPE NAME

ClassAction.org
