EXHIBIT 1

This notice will be supplemented should any new significant facts be learned subsequent to its submission. By providing this notice, University of Pennsylvania ("the University") does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On March 22, 2024, Educational Computer Systems, Inc ("ECSI"), a third-party vendor, advised its client, the University, of an unusually high volume of access attempts on one of its online services. This service, provided on behalf of clients such as the University, allowed students and borrowers to access tax forms online without logging into a user profile. Upon discovery of the event, ECSI advised that it took the service offline, launched an investigation with the assistance of third-party cybersecurity specialists and notified law enforcement. ECSI advised that its investigation determined an unauthorized individual accessed information relating to certain student or borrower tax forms between October 29, 2023, and February 12, 2024.

The information that could have been subject to unauthorized access includes individuals' name and Social Security number.

Notice to Maine Resident

On or about April 9, 2024, ECSI provided written notice of this incident on behalf of the University to one (1) Maine resident. Written notice was provided in substantially the same form as the letter attached here as ***Exhibit A***. On May 8, 2024, ECSI disclosed to the University that a resident of Maine was included in this population.

Other Steps Taken and To Be Taken

Upon discovering the event, ECSI advised the University that they moved quickly to investigate and respond to the incident, assess the security of its systems, and identify potentially affected individuals. Further, ECSI notified federal law enforcement regarding the event. ECSI is also working to implement additional safeguards and training to its employees. ECSI provided access to credit monitoring services for twenty-four (24) months, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, ECSI provided impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. ECSI also provided individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

The University is providing written notice of this incident to relevant state regulators, as necessary.

EXHIBIT A

Template for All U.S. States Other than Massachusetts

[Notice of Data Breach]

April [**], 2024

On behalf of Educational Computer Systems, Inc. ("ECSI"), I am writing to inform you about a recent incident that involved personal information about you. ESCI provides certain services, including tax document preparation services, to a college or university at which you are or once were enrolled. We regret that this incident occurred and take the security of student information seriously.

WHAT HAPPENED. On February 12, 2024, ECSI became aware of an unusually high volume of access attempts on one of our online services provided on behalf of our college or university clients that previously allowed students and borrowers to access tax forms online without logging into a user profile ("the guest tax search functionality"). We took quick and decisive action to contain the incident, including proactively and temporarily taking the service offline and removing the guest tax search functionality. We quickly launched an investigation with the support of a respected third-party cybersecurity firm. Based on our investigation, we believe that an unauthorized individual(s) accessed information relating to certain student or borrower tax forms, at certain times between October 29, 2023 and February 12, 2024.

WHAT INFORMATION WAS INVOLVED. We believe that an unauthorized individual(s) was able to access certain personal information relating to you. In particular, we believe that this incident involved information from a Form 1098-E or Form 1098-T that you previously received from a college or university. This document included, for example, your name, certain dollar amounts (such as amount of tuition paid, scholarships received, or student loan interest paid) and Social Security number.

WHAT WE ARE DOING. As noted above, upon learning of this incident, we immediately took steps to contain the incident, including promptly eliminating the guest tax search functionality, and launched an investigation with the support of a leading third-party cybersecurity firm. We are also alerting you to this incident, as well as providing you with an offer of complimentary credit monitoring.

WHAT YOU CAN DO. The following provides information about steps that you can take to protect against potential misuse of personal information.

As a precaution, we have arranged for you, at your option, to enroll in a complimentary two-year credit monitoring service. We have engaged Experian to provide you with a credit and identity monitoring service, which includes, among other things, credit monitoring and certain identity theft protection and resolution services, and up to $1 million in identity fraud loss reimbursement. You have until [date] to activate the free credit monitoring and identity theft protection and resolution service by using the following activation code: [***]. This code is unique for your use and should not be shared. To enroll, visit [website] or call [toll-free number]. Be prepared to provide your engagement number: [***].

You should always remain vigilant for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions. If you believe you have been a victim of tax fraud, be sure to report it immediately to the Internal Revenue Service (IRS) using the resources available at https://www.irs.gov/individuals/how-do-you-report-suspected-tax-fraud-activity.

In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement, including your state Attorney General, to report incidents of identity theft or to learn about steps you can take to protect

yourself from identity theft. To learn more, you can go to the FTC's website at www.ftc.gov/idtheft, or call the FTC at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from the nationwide credit reporting agencies. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax (800) 685-1111 P.O. Box 740241 Atlanta, GA 30374-0241 www.Equifax.com	Experian (888) 397-3742 P.O. Box 9701 Allen, TX 75013 www.Experian.com	TransUnion (800) 680-7289 Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19022-2000 www.TransUnion.com

You may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to verify your identity. You may place a fraud alert in your file by calling any of the nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

In addition, you can contact the nationwide credit reporting agencies at the numbers listed above to place a security freeze to restrict access to your credit report. You will need to provide the credit reporting agency with certain information, such as your name, address, date of birth and Social Security number. After receiving your request, the credit reporting agency will send you a confirmation containing a unique PIN or password that you will need in order to remove or temporarily lift the freeze. You should keep the PIN or password in a safe place.

You also have other rights under the Fair Credit Reporting Act ("FCRA"). For information about your rights under the FCRA, please visit: https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

FOR MORE INFORMATION. Please know that we regret any inconvenience or concern this incident may cause you. Please do not hesitate to contact our dedicated contact center at [toll-free number] if you have any questions or concerns.

Sincerely,

Educational Computer Systems, Inc.

IF YOU ARE A DISTRICT OF COLUMBIA RESIDENT: You may obtain information about avoiding identity theft from the FTC or the District of Columbia Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
http://www.ftc.gov/idtheft/

Office of the Attorney General
441 4th Street, NW
Suite 1100 South
Washington, DC 20001
(202) 727-3400
https://oag.dc.gov/

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
http://www.ftc.gov/idtheft/

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.oag.state.md.us

IF YOU ARE A NEW YORK RESIDENT: You may obtain information about security breach response and identity theft prevention and protection from the FTC or from the following New York state agencies:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.gov/idtheft

New York Attorney General
Consumer Frauds &
Protection Bureau
120 Broadway, 3rd Floor Suite 650
New York, NY 10271
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Albany, New York 12231
(800) 697-1220
www.dos.ny.gov

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.gov/idtheft

North Carolina Department of Justice
Attorney General Josh Stein
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.com

IF YOU ARE A RHODE ISLAND RESIDENT: The incident involved covered personal information relating to approximately [#] Rhode Island residents. You may contact state or local law enforcement to determine whether you can file or obtain a police report relating to this incident. In addition, you can contact the Rhode Island Attorney General at:

Office of the Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400
http://www.riag.ri.gov/