Rensselaer

General Counsel and Secretary of the Institute
Troy Bldg., Third Floor
Rensselaer Polytechnic Institute
110 8th Street, Troy, NY 12180-3590

p: (518) 276-3777
f: (518) 276-4061
cookc5@rpi.edu
www.rpi.edu

February 2, 2024

Office of the Attorney General
Consumer Protection Bureau
1 Granite Place South
Concord, NH 03301
(via email: DOJ-CPB@doj.nh.gov)

Re: Notification of Cybersecurity Incident Potentially Affecting New Hampshire Residents

Dear Madam/Sir:

I am writing on behalf of Rensselaer Polytechnic Institute (RPI) in connection with an incident that may have impacted the security of certain personal information of sixty-one (61) New Hampshire residents. RPI is reporting potential unauthorized access to this information.

RPI is an accredited university located in Troy, NY. On November 17, 2023, RPI's vendor, Athletic Trainer System (ATS), notified RPI that certain RPI student athlete and former student athlete data may have been compromised by a breach that occurred during the period from August 2020 to January 2021. ATS is a provider of software that RPI has used to store and manage student athlete injury information. We were informed the responsible party used a "data miner" tool to collect information from accounts with vulnerable passwords, that the FBI is prosecuting the perpetrator, and that RPI is one of many institutions that was impacted.

ATS provided us information on the potentially affected individuals in December 2023, and we investigated the matter, including attempting to obtain additional information from the FBI on the matter, speaking with ATS, and reviewing the information provided by ATS to determine which students' profiles contained personal information. While we understand that the perpetrator had access to personal information, we have no evidence as to which, if any, RPI students' information was actually downloaded, or whether any such information was transferred to anyone else.

The compromised ATS database contained profiles for a student's

Information actually stored in the database varied by student, however.

On February 1, 2024, RPI notified potentially affected individuals, including sixty-one (61) New Hampshire residents. Enclosed is the notification letter that was sent to those residents via email.

Please contact me should you have any questions or require additional information about this matter.

Sincerely,

Craig A. Cook
General Counsel and Secretary of the Institute

INFORMATION SECURITY/CISO
RENSSELAER POLYTECHNIC INSTITUTE

February 1, 2024

Dear RPI Student or Former Student:

I am writing to inform you of a data security incident involving Athletic Trainer System (ATS), a provider of software that RPI has used to store and manage student athlete injury information. Your personal information may have been compromised and I am providing you with details about the incident and our response, along with resources to help you protect your information.

What Happened?

On November 17, 2023, ATS notified RPI that student information stored on an ATS server was involved in a cyber incident that occurred between January 2020 and January 2021. After an investigation involving the FBI, we were informed the responsible party used a "data miner" tool to collect information from accounts with vulnerable passwords. The FBI is prosecuting the perpetrator, and RPI is one of many institutions that were impacted.

The compromised ATS database contained profiles for a student's

. Information actually stored in the database varied by student, however.

.

Protecting Your Data

It is unfortunate that we were not notified of this breach until November of 2023. Please know your privacy and the security of your information is a top priority at RPI, and we have taken steps to ensure the safety of student athlete information.

- All staff who have administrative access to this software have been required to change their passwords, use dual factor authentication for access, and ensure compliance with RPI's password complexity standards.
- RPI is transitioning to a new system called PyraMed and will no longer be using the ATS software.
- RPI is providing you with information on how you can implement fraud alerts and credit freezes with credit agencies and obtain free credit monitoring services. You'll find this information and additional resources in the accompanying "Steps You Can Take to Protect Your Information."

Rensselaer

INFORMATION SECURITY/CISO

RENSSELAER POLYTECHNIC INSTITUTE

Please rest assured that we are taking this incident very seriously, and we will continue to safeguard the information in our care. If you have questions or need additional information, you may contact us by calling our dedicated assistance line at 1-888-647-3744, Monday through Friday from 8:00am - 8:00pm ET (excluding major U.S. holidays) or email us at . You may also write to us at Rensselaer Polytechnic Institute, 110 8th Street, Troy, NY 12180 Attn: DotCIO, Troy Bldg. 4th Fl.

Sincerely,

Colleen Morrissey
Director, Information Security & CISO

INFORMATION SECURITY/CISO
RENSSELAER POLYTECHNIC INSTITUTE

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Monitor Your Accounts

Identity theft reporting information and resources can be found at www.identitytheft.gov. We strongly recommend that all individuals take the following steps to help protect against data and identity theft:

- Be aware of phishing and spam.
- Do not give out personal information, including responding to unknown emails, voice calls, and text messages.
- Do not reuse passwords across accounts.
- Enable MFA (multi-factor authentication) on all accounts where possible.
- Regularly check bank and credit card activity.
- If you notice any suspicious activity notify your providers immediately.
- Consider contacting the Social Security Administration at 1-800-772-1213 to block electronic access to your information.

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau. Additional steps you can take are as follows:

Enable Fraud Alerts. You have the right to place an initial or extended fraud alert on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

Place a Credit Freeze. You also have the right to place a credit freeze on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report.

Credit Monitoring. You may obtain credit monitoring from Experian at no cost to you. A description of such credit monitoring services is available on the Experian website identified below. You can also choose other credit monitoring or identity protection services at your cost.

Should you wish to place a fraud alert or credit freeze, or take advantage of no-cost credit monitoring, please contact the three major credit reporting bureaus listed below:

TransUnion	**Experian**	**Equifax**
1-800-680-7289 www.transunion.com	1-888-397-3742 www.experian.com	1-888-298-0045 www.equifax.com
TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000	Experian Fraud Alert P.O. Box 9554 Allen, TX 75013	Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069
TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
Fraud Alert: https://www.transunion.com/fraud-alerts Credit Freeze: https://www.transunion.com/credit-freeze	Credit Monitoring: https://www.experian.com/consumer-products/credit-monitoring.html Fraud Alert: https://www.experian.com/fraud/center.html Credit Freeze: https://www.experian.com/freeze/center.html	Fraud Alert and Credit Freeze: https://www.equifax.com/personal/credit-report services/

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. Dawson James Securities, Inc. may be contacted at 101 N. Federal Highway, Suite 600, Boca Raton, Florida 33432.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f7201504 cfl>b summary your-rights-under-fcra.pd (or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; l-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or l-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; l-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 15 Rhode Island residents impacted by this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and https://oag.dc.gov/consumer-protection.

Rensselaer Polytechnic Institute may be contacted at 110 8th Street, Troy, NY 12180 Attn: DotCIO, Troy Bldg. 4th Fl.