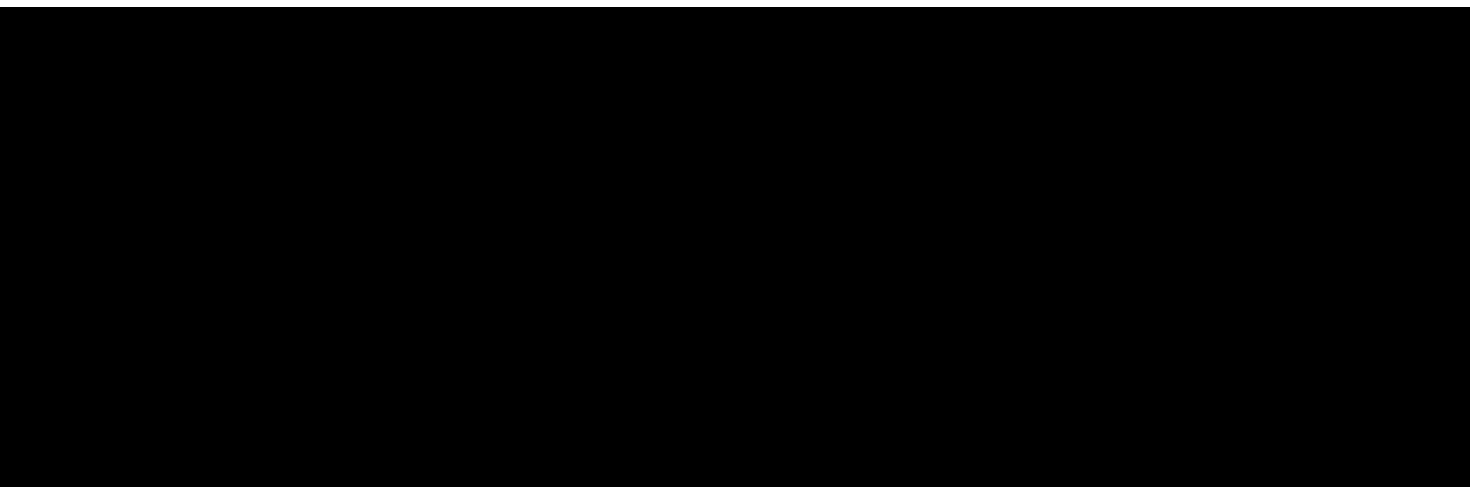




Hello,

On February 1, 2022, Pellissippi State Community College (PSCC) in Knoxville, Tennessee will be informing individuals of a recent data security incident that may have resulted in the unauthorized access to, or acquisition of, some personal information of our former and current students, faculty, and staff and participants in Tennessee Consortium for International Studies (TNCIS) programs. The attack occurred overnight on December 5-6, 2021. On January 13, 2022, we learned via preliminary analysis by our contracted cybersecurity consultant of the unauthorized access of one system. Based on the permanent address listed in our enterprise database, this includes 292 Maryland residents.

What Happened?

PSCC was the victim of a ransomware cyberattack overnight on December 5-6, 2021. We have confirmed unauthorized access to one system, but it is possible that others may have been accessed.

What Information Was Involved?

Our investigation confirmed that the attacker had access to our Active Directory database, which includes first and last name; PSCC username; PSCC email address; office location and phone number; job title and department (if an employee); P number (a unique number assigned to each student and employee used only at PSCC and not used to sign documents); General user ID number (a long random string of numbers used only by PSCC in its Banner system); and PSCC account password (hashed).

This was the only database to which access was confirmed. It is possible, however, that other personal data in our system could have been accessed.

What We Are Doing

Since the incident, we have notified local law enforcement, including the Tennessee Bureau of Investigation, and appropriate state and federal authorities, scanned every computer, and enhanced security measures.

Attached, in PDF format, is the text of the notification that will be sent on February 1, 2022. If you need additional information, please let me know.

Thank you,



Audrey J Williams

Audrey J Williams, MEd, MSIS

Vice President of Information Services/CIO

Pellissippi State Community College

10915 Hardin Valley Road • P.O. Box 22990 • Knoxville, TN 37933-0990 USA

865 539.7198

@ajwms

Pronouns: she/her/hers ([what is this?](#))



Dear First Name Last Name,

Pellissippi State Community College (PSCC) is informing individuals of a recent data security incident that may have resulted in the unauthorized access to, or acquisition of, some personal information of our former and current students, faculty, and staff and participants in Tennessee Consortium for International Studies (TNCIS) programs.

What Happened?

PSCC was the victim of a ransomware cyberattack overnight on December 5-6, 2021. We have confirmed unauthorized access to one system, but it is possible that others may have been accessed. While PSCC was also a victim, we apologize for any stress and concern this has caused.

What Information Was Involved?

Our investigation confirmed that the attacker had access to our Active Directory database, which includes first and last name; PSCC username; PSCC email address; office location and phone number; job title and department (if an employee); P number (a unique number assigned to each student and employee used only at PSCC and not used to sign documents); General user ID number (a long random string of numbers used only by PSCC in its Banner system); and PSCC account password (hashed). This was the only database to which access was confirmed. It is possible, however, that other personal data in our system could have been accessed.

What We Are Doing

Since the incident, we have notified local law enforcement, including the Tennessee Bureau of Investigation, and appropriate state and federal authorities, scanned every computer, and enhanced security measures.

What You Can Do

While we do not know if your data was viewed, we generally recommend you remain vigilant, monitor and review your financial and account statements, and report any unusual activity. More specifically, we recommend you:

- Reset passwords for any accounts that used the same password as was in our system (and use different passwords for different accounts);
- Notify your financial institution if you detect suspicious activity on your accounts;

NOTIFICATION FROM PELLISSIPPI STATE COMMUNITY COLLEGE – February 1, 2022

- Report incidents of fraudulent activity or suspected identity theft to proper law enforcement authorities, the Federal Trade Commission, and/or your state attorney general;
- Monitor your free credit reports;
- Consider placing a freeze on your credit files and/or a fraud alert on your credit report;
- File a police report if you experience identity fraud;
- Take advantage of the Federal Trade Commission's information at: [IdentityTheft.gov](https://www.identitytheft.gov) and Identity Theft | FTC Consumer Information; and
- Review the attached State-Specific and Other Important Information.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (myTrueIdentity) for 12 months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the myTrueIdentity website at www.mytrueidentity.com and in the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code **XXXXXXXXXX** and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the following 6-digit telephone pass code **#####** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft. You can sign up for the online or offline credit monitoring service anytime between now and May 31, 2022. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The subscription also includes access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

If you have questions about your online credit monitoring benefits, need help with your enrollment, or need help accessing your credit report, or passing identity verification, please contact the myTrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am-9pm, Saturday-Sunday: 8am-5pm Eastern time.

If you are receiving this notice for a current or former student who is under the age of 18:

The credit monitoring code listed above is only for adults. If you are receiving this notice for a minor, the parent or guardian can contact the call center listed below to receive a unique code for 12 months of credit monitoring specific for covering minors which will provide notifications to the primary adult member of activity on the child's Equifax credit report.

For More Information

PSCC sincerely regrets any inconvenience or concern that this attack on us caused. Additional information in the form of Frequently Asked Questions (FAQs) is available at <https://www.pstcc.edu/cyberattack>. If you still have questions after reading the FAQs and this notification, please contact the call center PSCC has established at 1-855-604-1808 This call center will be operational through May 2, 2022.

Please note that by providing this notice, PSCC does not intend to waive any rights or defenses.

State-Specific and Other Important Information

How do I obtain a copy of my credit report?

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <https://www.annualcreditreport.com>, by calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. Contact information is also provided below:

Experian P.O. Box 2104 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 2000 Chester, PA 19022 1-800-680-7289 www.transunion.com	Equifax P.O. Box 740256 Atlanta, GA 30348 1-888-766-0008 www.equifax.com
---	---	--

How do I place a security freeze on my credit report

You may place a security freeze on your credit report by contacting the credit reporting agencies below. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. Many states require the security freeze to be free of charge.

Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion P.O. Box 1000 Chester, PA 19016 1-888-9098872 www.transunion.com/credit-freeze	Equifax P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 www.equifax.com/personal/credit-report-services/credit-freeze/
---	--	--

How do I place a fraud alert on my account?

You can place fraud alerts by contacting the credit reporting agencies below. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	TransUnion P.O. Box 1000 Chester, PA 19016 1-888-9098872 www.transunion.com/fraud-alerts	Equifax P.O. Box 105788 Atlanta, GA 30348 1-888-298-0045 www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
---	--	--

What should I do if my family member's information was involved in the incident and is deceased?

We are sorry for your loss. To help protect your deceased family member, there are steps you can take to request a copy of your deceased family member's credit report. An executor or surviving spouse can place a request to any of the three credit reporting agencies for a copy of the deceased individual's credit report. An executor or surviving spouse can also request that the following two notices be placed on a deceased individual's credit report:

- "Deceased – Do not issue credit"
- "If an application is made for credit, please notify the following person(s) (e.g. surviving relative, executor/trustee of the estate and/or local law enforcement agency – notifying the relationship)."

For more information regarding identity theft and the deceased, please visit [Identity Theft and the Deceased: Prevention and Victim Tips | Office of Justice Programs \(ojp.gov\)](https://www.ojp.gov/identity-theft-and-the-deceased)

How do I contact the FTC?

To contact the FTC, you can send a letter to the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580; go to www.IdentityTheft.gov/databreach; or call 1-877-438-4338. Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement agencies.

District of Columbia Residents: You have the right to obtain a security freeze free of charge. You may contact the D.C. Attorney General at: 400 6th Street, NW, Washington, DC 20001, 202-727-3400, or Attorney General Karl A. Racine | Attorney General Karl A. Racine (dc.gov).

Maryland Residents: You may obtain information from the M.D. Attorney General, who can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, or Maryland Attorney General - Brian E Frosh.

Massachusetts Residents: You that you have the right to obtain a police report. You may also obtain a security freeze on your credit report free of charge. To do so, you will need the following information: your full name, Social Security number, address(es), date of birth, a copy of a government issued identification card, a copy of a utility bill, bank or insurance information, or anything else the credit reporting agency needs to place the security freeze.

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, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; and you must give your consent for credit.

New York Residents: You may contact the following state agencies for information regarding security breach response and identity theft prevention and protection information.

- Bureau of Internet and Technology, 28 Liberty Street, New York, NY 10005, 212-416-8433, Bureau of Internet and Technology (BIT) Resources | New York State Attorney General (ny.gov); and/or
- Department of State, Division of Consumer Protection, 800-697-1220, <http://www.dos.ny.gov/consumerprotection>
-

North Carolina Residents: You may wish to review the information provided by the North Carolina Attorney General at www.ncdoj.gov, or by contacting the Attorney General by calling 877-5-NO-SCAM (Toll-free within North Carolina) or by mailing a letter to the Attorney General at North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699.

Rhode Island Residents: You have the right to obtain or file a police report. Further, you can obtain information from the Rhode Island Office of the Attorney General: 150 South Main Street, Providence, RI 02903, 401-274-4400, www.riag.ri.gov. You have the right to place a security freeze on your credit report at no charge, but the consumer reporting agencies may charge fees for other services.