PENINSULA COLLEGE

July 26, 2023

Office of the Washington State Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-mail: securitybreach@atg.wa.gov

To the Washington State Office of the Attorney General,

Over the months of June and July 2023, the National Student Clearinghouse (NSC) and Teachers Insurance and Annuity Association (TIAA) emailed notification to Peninsula College (College), a Washington State Community and Technical College and state agency, that a secure file transfer system both companies employ called MOVEit, was exposed in a cybersecurity incident. Although the College's system was not breached, the College has reason to believe that NSC's use of the MOVEit software exposed its students' sensitive personal information and TIAA's use of the MOVEit software exposed employees' personal information. The College seeks to protect those students and employees.

NSC Cybersecurity Incident
This is what the College understands the situation to be right now:

NSC is a major clearinghouse for many if not all institutions of higher education. They are used for transcript verifications, enrollment data, financial aid, among other services. The cybersecurity incident involving MOVEit software exposed thousands of students nationwide.

On or around May 30, 2023, an unauthorized third party took NSC data residing on the MOVEit transfer software. On June 16, 2023, NSC sent The College a notice of a possible data alert. On June 30, 2023, NSC sent a notification, dated two days prior, confirming it believed The College's data was implicated in the cybersecurity incident, however they do not know what information was taken nor from whom. NSC has sent several notices informing The College it is working with law enforcement and investigating the scope of the breach, and that they expect to know what information was exposed in the upcoming weeks.

The College has a contract with NSC that requires NSC to remediate and mitigate any potential damage caused by the cybersecurity incident. NSC is responsible for investigation into the cause of the breach; providing notification of the cybersecurity incident as required by law; providing credit file or identity monitoring; and operate an identity theft call center to respond to questions from students whose personal information may have been accessed or disclosed.

PENINSULA COLLEGE

TIAA Incident
TIAA is a vendor that houses information of employees at The College. On June 29, 2023, The College received an email from TIAA, confirming that employees' personal information was involved in a third-party data security incident. The incident involves the MOVEit Transfer software owned by Progress Software and used by TIAA's vendor, Pension Benefit Information, LLC (PBI). PBI receives personal data of individual participants and clients and matches it against death notices and obituaries to assist TIAA in death claims and beneficiary processes. At this time, The College has not been informed as to the number of employees' whose data has been implicated in the incident.

The number of Washington Residents Affected:
The exact number of residents exposed by the NSC breach is unknown. Due to the notice from NSC dated June 28, 2023, The College began investigating our recent upload of information (performed May 30, 2023). The College is concerned that 1,413 student records could have been impacted due to the information contained in the May 30, 2023, upload.

The exact number of residents exposed by the TIAA third party incident is unknown.

The College will not know that true number until NSC and TIAA releases that information in the upcoming weeks.

A list of the personal information that were or are reasonably believed to have been subject of a cybersecurity incident:
The College uploaded the following data to NSC around the time of the cybersecurity incident:

- Name
- Address
- Social Security Number
- Student identification number
- Enrollment information

The College understands the following data on the MOVEit Software used with TIAA's third party vendor could have access to the following information:

- First and last name
- Address
- Date of birth
- Gender
- Social Security Number

The College has no certainty as to what information was taken, whether it was encrypted in a secure manner, or whether it was segregated. The College sends this notice in an abundance of caution.

PENINSULA COLLEGE

Timeframe of exposure:
NSC reports that the exposure occurred in late May. The College has no information on when the TIAA breach occurred but believes it to be at the same time because both institutions utilize the MOVEit software. The College is working to ascertain more specifics.

A Summary of the Steps taken:
The College assembled an incident response team. The team has been working with its Attorney General on understanding legal obligations. It has investigated tools available for responding to the security incident. The College also took the following specific actions:

1. On July 20, 2023, The College published a website informing students of what occurred and what they can do to protect themselves. Third Party Cybersecurity Incident Impacts Peninsula College Community | Peninsula College (pencol.edu)
2. On July 21, 2023, The College informed the local media of the cybersecurity incident. The local newspaper circulated an article on the incidents and what students affected can do.
3. On July 25, 2023, The Attorney General's Office in Port Angeles mailed and emailed a demand for more information and commitments from NSC.
4. Peninsula College designated contact persons for NSC per their request. They have signed up for updates and Peninsula College is tracking the situation as it waits for more specifics.

The College is in the information gathering stage. The College is still awaiting a list of who was and what was exposed and a copy of the notice NSC and TIAA are planning to send to impacted individuals.

The College has heard Pension Benefit Information (PBI) LLC, TIAA's third party vendor, has agreed to provide 24 months of credit monitoring at no cost to the impacted individuals. The College awaits direct confirmation of this.

Copies of the notice to be sent:
NSC has not provided The College with a copy of their notice. The College has requested this information and plans to hold NSC accountable for performance on their contract with Peninsula College.
Attached is a notice from Washington State Board for Community and Technical Colleges that will be sent to impacted employees. The College does not have the notice sent by PBI as written in this attached notice.

The College will be asking both entities to include the information requisite under RCW 42.56.590(6)(a).

Conclusion
Peninsula College may be the first state agency notifying the Attorney General's office under RCW 42.56.590 of the MOVEit incident. This is because Peninsula College was able to determine it was transferring personal information potentially impacting over 500 Washington residents at the time of the

breach through its data records. In an abundance of caution, Peninsula College believes it to be prudent to inform the Attorney General's Office of this cybersecurity incident.

Should you have any questions regarding this notification or other aspects of the data security event, please contact:

National Clearing House – MOVEit Incident
Krista Francis, Vice President of Student Services
kfrancis@pencol.edu 360-417-6225

Teachers Insurance and Annuity Association – MOVEit Incident
Hanan Zawideh, Vice President of Human Resources, Diversity, Equity, Inclusion
hzawideh@pencol.edu 360-417-6212

Sincerely,

Carie Edmiston

Carie Edmiston
Vice President for Finance and Administration
cedmiston@pencol.edu
360-417-6205

Enclosure:
SBCTC Email Notice to impacted employees
regarding TIAA incident

Dear _____,

TIAA is a financial organization that offers investment and insurance services to employees working in the academic, research, medical, governmental, and cultural fields. TIAA is one of the employee retirement benefit plan providers to the Washington State Board for Community and Technical Colleges (SBCTC) and its 34 colleges.

TIAA uses a third-party vendor, Pension Benefit Information (PBI) LLC, to implement certain beneficiary processes. TIAA notified SBCTC that PBI was impacted by the MOVEit security incident.

As we understand it, the data security incident resulted in the exposure of your first and last name, address, date of birth, gender, and social security number to an unauthorized actor.

PBI has agreed to provide 24 months of credit monitoring at no cost to you. You should have received a letter by mail from PBI with instructions and a unique code to reference when registering for the free credit monitoring. The letter from PBI also will include contact information to learn more or ask questions about the credit monitoring service. Please refer to the details from PBI to avail yourself of credit monitoring and any additional information related to this incident.

If you have not received a letter, please contact the PBI assistance line at 866-373-9043 (9 a.m. to 6:30 p.m. Eastern time, excluding holidays) or write to:

Pension Benefit Information (PBI)
333 South Seventh Street, Suite 2400
Minneapolis, MN 55402

Sincerely,

Julie Huss (she, her, hers)
Human Resources Director
Washington State Board for Community and Technical Colleges
jhuss@sbctc.edu • o: 360-704-4350
sbctc.edu • Twitter: @SBCTCWashington • Facebook: @WASBCTC

From: Kari Desser
Subject: Third Party Cybersecurity Incident Impacts Peninsula College Community
Date: Thursday, July 20, 2023 12:04:15 PM
Attachments: 7.20.23 Talking Points for Frontline Workers re Third Party Cybersecurity Incident.docx
image001.png

PENINSULA COLLEGE

NEWS RELEASE

FOR IMMEDIATE RELEASE: July 20, 2023

CONTACT: Kari Desser, kdesser@pencol.edu

Third Party Cybersecurity Incident Impacts Peninsula College Community

Port Angeles, WA. –Two vendors have notified Peninsula College of a cybersecurity incident that may have exposed personally identifiable information of current students as well as employees.

At issue is the popular filesharing application MOVEit Transfer used by hundreds of businesses and organizations worldwide. PC does not use the MOVEit software, though two of the college's vendors do and have contacted the college about the potential exposure of personally identifiable information.
The college has set up a website with more information on the incident, which will update as more details become available.

The two vendors that have contacted Peninsula College are the National Student Clearinghouse (NSC) and the Teachers Insurance and Annuity Association (TIAA).

PC contracts with NSC on a number of endeavors, including enrollment and degree verification services as well as student loan reporting requirements. The National Student Clearinghouse is a nonprofit organization that provides educational reporting, data exchange, and verification services to more than 3,600 colleges and universities nationwide. Personally identifiable information and student education records are provided to NSC as part of this work.

Additional details about the incident are available on NSC's website.

TIAA offers financial services to employees across the country working in academic, research, medical, government and cultural fields. Peninsula College provides TIAA with personally identifiable information of employees who use TIAA's services. Data transferred from PC to TIAA was not

compromised as part of the incident, though the organization has indicated that Pension Benefit Information, LLC, one of its vendors, has been impacted.

For more information contact TIAA's National Contact Center 1-800-842-2252.

The college expects NSC and Pension Benefit Information, LLC, will contact impacted individuals directly, as required by law. The timeline of that notification is unknown.
Peninsula College is sending this message to inform students and employees so they can take steps to keep their identity as secure as possible. Any members of the PC community who believe their personal information may have been compromised are advised to follow the recommendations of the Federal Trade Commission:

- Closely monitor your credit reports.
    - You can obtain a free copy of your credit report from each of the three major credit reporting agencies; Equifax, Experian, and TransUnion.

- Place a fraud alert on your accounts.
    - A fraud alert tells creditors to contact you before opening any new accounts or before making changes to existing accounts. You can place a fraud alert by contacting one of the three credit reporting agencies. A fraud alert at one of the agencies will automatically notify the other two services.

- Freeze your credit at each of the three major credit reporting agencies.

- If you believe you are the victim of identity theft, file a police report and notify the Federal Trade Commission at www.identitytheft.gov.

- Block electronic access to your Social Security information.
    - Contact the Social Security Administration at 1-800-772-1213 to block electronic access. This will prevent anyone from being able to see or change your personal information on the internet or by the administration's automated telephone service.

PBI will send affected individuals a letter by mail in the coming weeks offering free credit monitoring for two years **at no cost to them**.

###