

July 27, 2023

Dear Office of the Attorney General,

This letter serves as the official notification (RCW 42.56.590(7)(a)) of a data breach incident that has impacted Tacoma Community College students and employees. Two third-party vendors have recently notified TCC of a cybersecurity incident that may have potentially exposed personally identifiable information of some students and employees.

The data breach took place with a software tool called MOVEit Transfer, which thousands of organizations across the world use to transfer files. TCC does not use MOVEit Transfer. TCC has partnerships with organizations such as the National Student Clearinghouse (NSC) and the Teachers Insurance and Annuity Association (TIAA) that do use MOVEit Transfer. Both NSC and TIAA recently notified TCC about the potential exposure of personally identifiable information of some students and employees.

It is important to note that no systems directly operated by TCC have been breached. This incident is localized to our third-party vendors, which includes MOVEit Transfer, NSC and TIAA.

TCC has notified the following affected groups:

- Students who were enrolled in spring and summer quarters.
- Employees
 - Including employees who have left the system
- The general community

We have attached the communications that we have shared with our constituents. All communications have been via email and we have deployed a website with more information (https://www.tacomacc.edu/about/newsroom/summer2023_spring2024/databreach).

We do not yet know the specific impacted individuals nor the specific details of what was breached. We have been in contact with NSC and evaluating our contract and insurance. We have asked NSC to notify the impacted individuals and ask to provide credit protection measures.

Once we receive additional information, we will supplement this notice with additional information (RCW 42.56.590(7)(b)).

Thank you.

XXXXXX

Notice to Washington Residents and/or Impacted Individuals

July 20, 2023

Website on [tacomacc.edu](https://www.tacomacc.edu):

https://www.tacomacc.edu/about/newsroom/_summer2023_spring2024/databreach

Notification to TCC employees:

Dear College Community,

Two third-party vendors have notified TCC of a cybersecurity incident that may have potentially exposed personally identifiable information of some students and employees.

The data breach took place with a software tool called MOVEit Transfer, which thousands of organizations across the world use to transfer files. TCC does not use MOVEit Transfer. TCC has partnerships with organizations such as the National Student Clearinghouse (NSC) and the Teachers Insurance and Annuity Association (TIAA) that do use MOVEit Transfer. Both NSC and TIAA recently notified TCC about the potential exposure of personally identifiable information of some students and employees.

It is important to note that no systems operated by TCC or SBCTC, including ctcLink, have been breached. This incident is localized to our third-party vendors, which includes MOVEit Transfer, NSC and TIAA.

The vast majority of higher education institutions around the country transfer data through the NSC to facilitate tasks such as financial aid compliance, transcripts and verification. All of Washington's 34 community and technical colleges use NSC in some capacity. However, not all of Washington's community and technical colleges have been affected by the data breach. NSC has recently contacted all of the state's affected colleges. And this breach has impacted many other institutions throughout the country.

As with all incidents like this, we take this situation very seriously. We are working closely with the State Board of Community and Technical Colleges to track this situation and conduct a report to help us determine the extent of the breach as well as research ways to protect ourselves from fraudulent activities. We also are working with the Attorney General's Office to address legal implications.

TCC expects NSC and TIAA to contact impacted individuals, as required by law. In the meantime, there are specific steps you can take:

- Monitor credit cards and bank accounts

- Place fraud alerts and credit freezes
- Do not open or click on links with any suspicious emails or texts
- Update passwords

We have launched a webpage with further tips and more information.

As more information becomes known, we will share with you.

Thank you.

July 24, 2023

Students – enrolled in spring and summer quarters – 1 credit+

Dear College Community,

Two third-party vendors have notified TCC of a cybersecurity incident that may have potentially exposed personally identifiable information of some students and employees.

The data breach took place with a software tool called MOVEit Transfer, which thousands of organizations across the world use to transfer files. TCC does not use MOVEit Transfer. TCC has partnerships with organizations such as the National Student Clearinghouse (NSC) and the Teachers Insurance and Annuity Association (TIAA) that do use MOVEit Transfer. Both NSC and TIAA recently notified TCC about the potential exposure of personally identifiable information of some students and employees.

It is important to note that no systems operated by TCC or SBCTC, including ctcLink, have been breached. This incident is localized to our third-party vendors, which includes MOVEit Transfer, NSC and TIAA.

The vast majority of higher education institutions around the country transfer data through the NSC to facilitate tasks such as financial aid compliance, transcripts and verification. All of Washington's 34 community and technical colleges use NSC in some capacity. However, not all of Washington's community and technical colleges have been affected by the data breach. NSC has recently contacted all of the state's affected colleges. And this breach has impacted many other institutions throughout the country.

As with all incidents like this, we take this situation very seriously. We are working closely with the State Board of Community and Technical Colleges to track this situation and conduct a report to help us determine the extent of the breach as well as research ways to protect ourselves from fraudulent activities. We also are working with the Attorney General's Office to address legal implications.

TCC expects NSC and TIAA to contact impacted individuals, as required by law. In the meantime, there are specific steps you can take:

- Monitor credit cards and bank accounts
- Place fraud alerts and credit freezes
- Do not open or click on links with any suspicious emails or texts
- Update passwords

We have launched a webpage with further tips and more information.

As more information becomes known, we will share with you.

Thank you.

July 26, 2023

News release – media

TCC Students, Employees May Have Been Impacted by Third-Party Data Breach

Two third-party vendors have notified Tacoma Community College of a cybersecurity incident that may have exposed personally identifiable information of some of the college's students and employees.

The data breach took place with a software tool called MOVEit Transfer, which thousands of organizations across the world use to transfer files. Although TCC does not use MOVEit Transfer, the college has partnerships with organizations, including National Student Clearinghouse (NSC) and the Teachers Insurance Annuity Association (TIAA), that use the service. Both NSC and TIAA recently notified TCC about the potential exposure if personally identifiable information of some students and employees.

No systems operated by TCC or the State Board for Community and Technical Colleges (SBCTC) have been breached. This incident is localized to our third-party vendors, including MOVEit Transfer, NSC, and TIAA.

The vast majority of higher education institutions around the country transfer data through the NSC to facilitate tasks such as financial aid compliance, transcripts and verification. All of Washington's 34 community and technical colleges use NSC in some capacity. However, not all of Washington's community and technical colleges have been affected by the data breach. NSC has recently contacted all of the state's affected colleges. This breach has also impacted many other institutions throughout the country.

"TCC takes the security of its student and employee data very serious," said Vice President for Administrative Services Patty McCray-Roberts. "We are working closely with the State Board for Community and Technical Colleges to track this situation, determine the extent of the breach, and research ways to protect ourselves from fraudulent activities. We are also working with the Washington State Attorney General's Office to address legal implications."

TCC expects NSC and TIAA to contact impacted individuals, as required by law. In the meantime, if you believe your data may be at risk, there are specific steps you can take:

- Monitor credit cards and bank accounts
- Place fraud alerts and credit freezes
- Do not open or click on links with any suspicious emails or texts
- Update passwords

[TCC has launched a webpage](#) with further tips and links to more information. The page will be updated as more information becomes known.