Published on *University of Colorado* (https://www.cu.edu)

MOVEit Software Cyberattack [1]

Dear CU Community Members,

Recently, a few of CU's vendors notified CU that they were impacted by the global cyberattack against the MOVEit Transfer software owned by Progress Software. What is currently known is that the cyberattack involves data for some in the CU community and includes prospective students, students, current employees and former employees. The cyberattack involved the following vendors:

1. **National Student Clearinghouse (NSC).** NSC provides educational reporting and research services to many higher education institutions. NSC used the MOVEit Transfer software and has indicated that CU student data was impacted. For more information visit: https://alert.studentclearinghouse.org/ [2]
2. **TIAA and Pension Benefit Information (PBI).** TIAA, CU's retirement plan recordkeeper, uses PBI to assist TIAA in death claim and beneficiary processes. PBI used the MOVEit Transfer software and has indicated that some CU participant data was impacted. For more information visit: https://www.pbinfo.com/faq-consumer/ [3]
3. **United Health Care Student Resources (UHCSR).** UHCSR provided student health insurance to CU Anschutz Medical Campus students and provides student health insurance to CU Denver international students. UHCSR used the MOVEit Transfer software and has indicated that data from CU students who enrolled in the UHCSR health insurance plan was impacted. For more information visit: www.uhcsr.com/media/dbd8af76-4e09-4bd1-b94c-eb94a4b4fdc6 [4]

Due to the nature of the software and how it was used by our vendors, individuals are unlikely at this time to know whether their personal data were impacted. If your personal data is included in the exposure, you will be notified in the near future. To take proactive steps to

protect your identity, learn more about actions you can take at https://www.identitytheft.gov/databreach [5].

Although this cyberattack happened to third-party vendors, it is a reminder of the importance of cybersecurity at CU. If you have questions about keeping data safe, please contact your campus/system administration information security office (https://www.cu.edu/security/about [6]).

We also 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 annualcreditreport.com [7] 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.

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.

As an alternative to a fraud alert, you 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.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion
1-800-680-7289
http://www.transunion.com [8]
Experian
1-888-397-3742
http://www.experian.com [9]
Equifax
1-888-298-0045
http://www.equifax.com [10]

We will continue to update the CU community on further developments.

FAQs (Frequently Asked Questions)

General

What occurred with this global cybersecurity event?
Progress Software disclosed that a critical vulnerability existed in their MOVEit Transfer software, which could result in unauthorized access of data in the files transferred by the software. A group of cybercriminals, CLOP, was able to exploit the vulnerability and gain access to companies' and institutions' data.

What is the MOVEit software used for?
MOVEit is a secure file transfer software for the handling of sensitive information utilized by many companies around the world.

Were University of Colorado systems impacted?
This cybersecurity event did not impact CU networks or systems. However, two vendors CU has a relationship with were impacted, Teachers Insurance and Annuity Association of America (TIAA) and the National Student Clearinghouse (NSC).

Were UHCSR systems impacted?
UHCSR has confirmed they use the MOVEit software and that they were impacted.

What does CU use UHCSR for?
UHCSR provided student health insurance for students at the CU Anschutz Medical Campus and currently provides student health insurance for international students at CU Denver.

How will I know if I am impacted by the UHCSR cyberattack?
If your personal data was impacted, you will receive a notification letter from UHCSR. UHCSR is also offering those impacted two years of complimentary credit monitoring and identity protection services. An explanation of how to access the free services will be provided in your written notification.

I am a student at the CU Anschutz Medical Campus. Isn't Anthem Student Advantage and not UHCSR providing student health insurance?
Anthem Student Advantage is providing student health insurance to CU Anschutz Medical Campus students beginning August 1, 2023. Previously, UHCSR was the student health insurance provider. If you were enrolled in the UHCSR student health insurance plan prior to August 1, 2023, your data may have been impacted. If you were not previously enrolled in the UHCSR student health plan, your data was not impacted. For more information about Anthem Student Advantage and student health plan enrollment information for the upcoming academic year at the CU Anschutz Medical campus visit:
https://www.cuanschutz.edu/student/health-wellness/student-health-insura... [11]

TIAA /PBI

Were TIAA systems impacted?
TIAA has confirmed their systems were not impacted, but a vendor they use, Pension Benefit Information (PBI), was impacted.

What does TIAA use PBI for?
PBI is a national company that audits death records to identify retirees and beneficiaries who have died.

How will I know if I am impacted by the TIAA / PBI cyberattack?
If your personal data was impacted, you will receive a notification letter from PBI. PBI is also offering those impacted free credit monitoring services. An explanation of how to access the free services will be provided in your written notification.

Were NSC systems impacted?
NSC has confirmed they use the MOVEit software and that they were impacted.

What does CU use NSC for?
NSC provides educational reporting and research services to higher education institutions as well as enrollment and degree verification services.

How will I know if I am impacted by the NSC cyberattack?
If your personal information was impacted by the NSC cyberattack, you will receive a written notification and free credit monitoring services, as required by law. CU is working with the vendor and will update this website once the process of notification is confirmed. NSC also has a website for updates and general information at https://alert.studentclearinghouse.org/ [2]

Identity Protection

What can I do to protect myself and my family?

- To learn more about proactive steps you can take to protect your identity, visit https://www.identitytheft.gov/databreach [5].
- We also 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 annualcreditreport.com [12] or call 1-877-322-8228.
- 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.
- 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.

Campus Contacts

CU Boulder
OITHelp@colorado.edu [13]
website [14]
CU Denver / Anschutz
oit-servicedesk@ucdenver.edu

[15]
website [16]

UCCS

security@uccs.edu [17]
website [18]

System Administration

security@cu.edu [19]
website [20]

Source URL:https://www.cu.edu/moveit-software-cyberattack

Links

[1] https://www.cu.edu/moveit-software-cyberattack [2] https://alert.studentclearinghouse.org/ [3] https://www.pbinfo.com/faq-consumer/ [4] http://www.uhcsr.com/media/dbd8af76-4e09-4bd1-b94c-eb94a4b4fdc6 [5] https://www.identitytheft.gov/databreach [6] https://www.cu.edu/security/about [7] http://www.annualcreditreport.com [8] http://www.transunion.com [9] http://www.experian.com [10] http://www.equifax.com [11] https://www.cuanschutz.edu/student/health-wellness/student-health-insurance [12] http://www.annualcreditreport.com/ [13] mailto:OITHelp@colorado.edu [14] https://oit.colorado.edu/services/it-security [15] mailto:oit-servicedesk@ucdenver.edu [16] https://www1.ucdenver.edu/offices/office-of-information-technology/secure-campus [17] mailto:security@uccs.edu [18] https://www.uccs.edu/oit/security [19] mailto:security@cu.edu [20] https://www.cu.edu/security