July 28, 2023 – 4:30 p.m.

The Virginia Community College System is Monitoring Two Vendor Cyberattacks

The Virginia Community College System (VCCS) is monitoring a nationwide cyberattack involving a third-party file transfer software tool called MOVEit Transfer used by vendors of the VCCS. The cybersecurity event involved hundreds of organizations and companies, including the National Student Clearinghouse (NSC), the Teachers Insurance and Annuity Association (TIAA), and Corebridge Financial (Corebridge). **This cybersecurity incident may have resulted in unauthorized access to personal information of students and employees of the VCCS.**

Upon learning of this software security vulnerability, the NSC, TIAA, and Corebridge took steps to secure their systems. Internal investigations and an FBI investigation are ongoing. Customers of TIAA and Corebridge will receive information about the data breach from Pension Benefit Information, LLC, the audit and research services company for TIAA, or Corebridge.

No systems operated, managed, or maintained by the VCCS have been breached or compromised in any manner.

The NSC determined an unauthorized party obtained certain data files transferred through the MOVEit Transfer product, including data files containing personal information that the NSC maintains on behalf of educational institutions. NSC believes the data files were obtained by the unauthorized party on or around May 30, 2023. NSC immediately began their investigation after learning of the vulnerability on May 31, 2023.

The cyberattack compromised personally identifiable information affecting VCCS along with thousands of businesses, government agencies, educational institutions and other organizations worldwide.

The NSC is a nongovernmental organization and a leading provider for enrollment reporting and verification data serving as a data exchange for many colleges and universities in the United States. The NSC also plays a role in managing student loan deferrals. Institutions are authorized to provide information to the NSC in connection with financial aid administration under the Family Education Rights and Privacy Act (FERPA). Student data is sent to the NSC for the National Student Loan Data System (NSLDS) as required by the U.S. Department of Education.

The extent of the cyberattacks is still not known and they are being fully investigated by the FBI and global cyber security experts. The VCCS is providing this information to keep our students informed. We encourage you to remain vigilant by monitoring bank accounts and credit records.

Actions Being Taken

The VCCS is actively monitoring the situation and working closely with NSC to identify any students who have been affected by this cybersecurity incident. To protect student data from further unauthorized access, the NSC has implemented a new, secure data transfer environment that was never accessed by the unauthorized third party.

As the investigation continues VCCS will continue to share information on this webpage. Since the breadth of the data compromised is still unknown, this alert will be posted on all 23 of our community college websites.

If your data was compromised, you will be contacted by NSC. To learn more from NSC and the actions they are taking visit www.alert.studentclearinghouse.org .

What You Can Do

VCCS takes data privacy and information security very seriously and we are working with NSC to determine the impact. Since the extent is still unknown, we encourage you to remain vigilant about potential indications of identity theft over the next 12 to 24 months and report suspected identity theft incidents to your institution and, if appropriate, law enforcement authorities.

Here are some actions you can take:

- Be extra vigilant:
  It is possible that cybercriminals may leverage stolen personal information from this attack to craft convincing phishing attacks in the coming weeks and months. An email, notice, or text message containing accurate information about you or one of your accounts is not enough to verify authenticity. Verify the source of a message before responding. Take note of how to identify a phishing attack. Phone calls may also be used to obtain personal or financial information.

- Monitor your financial accounts and credit:
  It is always wise to monitor your credit report for unusual activity. Consider putting a credit freeze in place to frustrate would-be scammers if you believe you are being targeted.

- Secure your accounts:
  Remember to enable two-factor authentication and to use long passphrases for all of your accounts. Never give someone your password or a two-factor code if asked for it, even if they claim to be from a trusted organization.

The Federal Trade Commission (FTC) provides useful information to help protect from identity theft at www.FTC.gov/IdTheft. If you find your personal information has been misused, visit the FTC's site at www.IdentityTheft.gov to report the identity theft and get recovery steps.

The investigation is ongoing and limited information is known. We will continue to post updates as we learn more about the breadth of the cyberattack. Please continue to check this webpage for updated information.