Incident Informational Bulletin

MOVEit Transfer Security Incident

What happened?
The National Student Clearinghouse (NSC) uses MOVEit Transfer, a third-party file transfer tool that was involved in a recent global cybersecurity incident, to transfer student data as it provides services to higher education institutions. On May 31, 2023, the NSC learned that the MOVEit Transfer product had a vulnerability and that an international cybercrime group exploited this security weakness and stole data held by public and private organizations around the globe, including the NSC. In the attack, education records about CSCU students were stolen from the NSC. Most individuals affected were individuals who were registered as students from the 1990s up to the past academic year (2022-23). Information that was stolen included names, contact information, and education record data such as enrollment, degree, and course-level data. For eighteen CSCU students, social security numbers (SSNs) and/or dates of birth were also acquired. The eighteen students whose SSNs or birthdates were stolen have been notified and have received offers of identity theft protection for two years as required by Connecticut state law.

How is the situation being handled?
The NSC immediately engaged federal support including the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and hired Kroll, a cybersecurity firm to assist with the investigation. The NSC also rebuilt their internal MOVEit Transfer data system and created a completely new environment for future work.

CSCU has been working with the NSC throughout this process to understand how CSCU students have been affected. Unfortunately, the NSC was unable to provide CSCU with information about which data elements were stolen for which students. In addition, the NSC did not provide CSCU with enough information about the affected students to find contact information for communication purposes. Since most affected students were registered in the past, the contact information that CSCU has on file is likely outdated making communication through postal or email addresses impossible.

CSCU will stay in communication with the NSC if additional information about the affected students is discovered or if there is evidence of misuse of the stolen data. In the meantime, CSCU is posting this information about the incident on its website for those who are seeking information.

What is the risk to me?
It is disconcerting to think that an international organization acquired information about individuals who have attended our CSCU institutions; however, we have no information that any use has been made of this information. CSCU works with a firm that scans the dark web for any activity related to CSCU email addresses, and there have been no negative reports to date. The risk of direct fraud or identity theft is low because additional information about the affected individuals would be needed. Even though the immediate risk of harm is low, the stolen information may exist with the perpetrator, be on the dark web for years to come, or be repurposed in the future. Because of this future risk, CSCU recommends establishing good data privacy and security habits. Please see the next section labeled "What should I do if I'm concerned?"

What this means for CSCU institutions?
No systems operated or maintained by CSCU were breached. We are providing this information so everyone in our community can take steps to protect their personal information since this incident had a broad impact. CSCU takes data privacy and information security seriously.

What should I do if I'm concerned?
Best practices for avoiding harm from the stolen data include the following standard guidance.

- Be extra vigilant.
- Use strong passwords and change them frequently.
- Enable two-factor authentication for your accounts when offered.
- Never share passwords or a two-factor code if asked, even if they claim to be from a trusted organization.
- Don't open suspicious email messages. Be alert to phishing and spoofing.
- Don't click on attachments in messages unless you are certain you know the sender.
- Minimize the information you post about yourself on social media that could be scraped and combined with other data about you on the dark web.
- Be alert for fraudulent activity on your credit card or financial accounts. Set up automatic alerts if offered.
- Never give out personal financial or account information over the phone unless you have initiated the contact and are certain that the individual receiving the information needs it for a legitimate purpose.
- Consider signing up for identity theft protection.
- Check your credit reports regularly. Everyone is eligible for one free credit report annually.

Why does my institution send data to the National Student Clearinghouse (NSC)?
The National Student Clearinghouse (NSC) provides postsecondary institutions in the United States (US) with automated enrollment verification and loan deferment reporting for financial aid students to the education lenders and the US Department of Education. Because processing of financial aid requires verification of enrollment, postsecondary institutions across the nation including all the Connecticut State Colleges and Universities (CSCU) send enrollment data to the NSC on a regular basis so that the NSC can provide enrollment status and deferment information to guarantee agencies, lenders and the US Department of Education's National Student Loan Data System (NSLDS). For more information about how the NSC's Enrollment Reporting system work, visit the NSC website:
https://www.studentclearinghouse.org/colleges/enrollment-reporting/faqs/

For more information
These resources may be helpful. In addition, you may contact the Data Privacy Officer with your questions at CSCU-DataPrivacy@ct.edu.

- The NSC's MOVEit Transfer Security Issue Update: https://alert.studentclearinghouse.org/
- US Government Cybersecurity & Infrastructure Security Agency MOVEit Transfer Vulnerability Report: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a