**Statement on National Student Clearinghouse Data Breach**

Lincoln University of Missouri has recently been made aware of a data breach within the National Student Clearinghouse (NSC). Lincoln is one of hundreds of higher education institutions that use NSC and its software MOVEit Transfer to share enrollment data with employers, lenders, etc. Upon learning of the vulnerability, NSC promptly launched an investigation and took steps to secure its MOVEit environment, including implementing patches to its MOVEit software. NSC reported the issue to law enforcement and has been working with leading cybersecurity experts to understand the issue's impact on its organization and systems. No systems operated or maintained by Lincoln were breached. This week, we have learned that 1,364 of Lincoln's students may have been affected by the breach.

NSC has assured Lincoln that no sensitive personal information such as social security numbers, birth dates, or transcript data was leaked. The types of personal information leaked included names, contact information, and educational information.

Again, while Lincoln has assurance from NSC that there is very little risk of identity theft for those who might have been affected, Lincoln still suggests students be diligent in taking the following precautions:

- Learn the signs of identity theft from the Federal Trade Commission at https://www.identitytheft.gov/.
- Check individual credit reports annually. Credit reports can be obtained for free at https://www.annualcreditreport.com.
- Monitor individual financial accounts (bank accounts, credit cards, investments, etc.)
- Consider signing up for an identity theft protection service.
- Consider placing a credit freeze on the credit report with each of the three credit-reporting agencies. https://consumer.ftc.gov/articles/what-know-about-credit-freezes-fraud-alerts?utm_campaign=376734_Notice%20of%20potential%20data%20breach%20-%20UM%20System%20Employees&utm_medium=email&utm_source=The%20Curators%20of%20the%20University%20of%20Missouri&dm_i=7IQU,82OU,3GW48W,15LC5,1
- Remain suspicious of any emails coming from unknown individuals or any emails with attachments or requests to click on links.
- Do not share personal information on email, social media posts, or in other electronic formats. That information might include passwords, Social Security numbers, and financial account information.

It is important to remember that even if every precaution is taken, individuals can still be victims of a crime. Anyone who thinks they might be a victim of a crime, such as fraud or ID theft, is encouraged to file a police report.

The NSC breach is still under investigation and is expected to take some time due to the number of schools and students involved. Stay informed of the latest information from NSC at https://alert.studentclearinghouse.org/.