National Student Clearinghouse®

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<Date>> (Format: Month Day, Year)

NOTICE OF DATA BREACH

Dear <<First_Name>> <<Last_Name>>,

We are writing on behalf of <<data owner name>> to notify you of an issue that involves your personal information. As you may be aware, National Student Clearinghouse (the "Clearinghouse") provides educational reporting and verification services to educational institutions, students and alumni, employers, and other organizations.

What Happened?

On May 31, 2023, the Clearinghouse was informed by our third-party software provider, Progress Software, of a cybersecurity issue involving the provider's MOVEit Transfer solution. MOVEit Transfer is a file transfer tool used by many organizations, including the Clearinghouse, to support the transfer of data files. After learning of the issue, we promptly initiated an investigation with the support of leading cybersecurity experts. We have also coordinated with law enforcement. Through our investigation, on June 20, 2023, we learned that an unauthorized party obtained certain files from the MOVEit tool. The issue occurred on or around May 30, 2023.

What Information Was Involved?

The relevant files obtained by the unauthorized third party included personal information such as name, date of birth, contact information, Social Security number, student ID number, and certain school-related records (for example, enrollment records, degree records, and course-level data). The data that was affected by this issue varies by individual.

What We Are Doing

We take the safeguarding of our systems and your data extremely seriously, and we have implemented patches to the MOVEit software pursuant to Progress Software's instructions and put in place additional monitoring measures to further protect our systems and your data. Additionally, we have arranged to offer identity monitoring services to you for two years at no cost to you.

What You Can Do

We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports for suspicious activity. The enclosed "Additional Resources" section provides information on ordering your free credit reports, registering for identity monitoring services and additional recommendations on the protection of your personal information.

For More Information

If you have any questions regarding this matter, please call **[insert toll-free number]**, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays. Please have your membership number ready.

We sincerely regret any inconvenience this may cause you.

Sincerely,

Ricardo D. Torres, President & CEO

Additional Resources

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Register for Identity Monitoring Services. We have arranged with Kroll to offer you identity monitoring services for two years at no cost to you. These services include:

- *Single Bureau Credit Monitoring*: You will receive alerts when there are changes to your credit data. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.
- *Fraud Consultation*: You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you ways to protect your identity, explaining your rights and protections, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.
- *Identity Theft Restoration*: If you become a victim of identity theft, a Kroll licensed investigator will work on your behalf to resolve related issues.

To take advantage of your identity monitoring services, please follow these instructions:

Visit **<<IDMonitoringURL>>** to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

Membership Number: [redacted]

For more information about Kroll and these services, you can visit info.krollmonitoring.com. Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your relevant financial institution or payment card company. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit https://www.identitytheft.gov/.

- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-525-6285
Experian, PO Box 9554, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-680-7289

Consider Placing a Security Freeze on Your Credit File. You may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually*. There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require you to provide certain personal information and proper identification prior to honoring your request to place a security freeze on your account. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver's license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

For Iowa Residents. You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at: 1305 E. Walnut Street, Des Moines, IA 50319; 1-515-281-5164; www.iowaattorneygeneral.gov

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For Massachusetts Residents. You have the right to obtain a police report and request a security freeze as described above.

For Minnesota Residents. You may request a report on the facts and results of the investigation into this incident by emailing privacy@studentclearinghouse.org.

For New Mexico Residents. You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or www.ftc.gov.

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Attorney General at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755 or 1-800-788-9898; https://ag.ny.gov/. You also may contact the Bureau of Internet and Technology (BIT), 28 Liberty Street, New York, NY 10005; 212-416-8433; https://ag.ny.gov/about/about-office/economic-justice-division#internet-technology.

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6400; www.ncdoj.gov

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; 1-877-877-9392 or 1-503-378-4400; www.doj.state.or.us

For Rhode Island Residents. You may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; www.riag.ri.gov. You have the right to obtain a police report and request a security freeze as described above.

For Washington, D.C. Residents. You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at: 400 6th Street NW, Washington, D.C. 20001; (202)727-3400; www.oag.dc.gov