Notice of Data Security Incident

Updated: [July 1, 2026]

Nelson University is committed to protecting the privacy and security of the personal information we maintain. We are making individuals aware of an incident that may affect the privacy of certain individuals' information. We are providing notice of the incident so that potentially affected individuals may take steps to protect their information, should they feel it appropriate to do so.

What Happened? On or around April 6, 2025, Nelson University detected potential unauthorized activity on our network. After identifying this, we took steps to evaluate and ensure the security of our systems and operations. Further, we engaged third-party independent cybersecurity experts to conduct an investigation into the incident.

Our investigation revealed that an unauthorized actor accessed our systems from on or about March 21, 2025, to on or about April 6, 2025, and, as a result, possibly viewed and/or obtained certain files from our network. We have been in the process of conducting an exhaustive review to identify the individuals whose personal information was included within the impacted data. This process concluded on May 26, 2026. To date, we have no evidence of financial fraud or identity theft arising out of the incident. Out of an abundance of caution, we are providing notice of the incident to individuals whose information was potentially impacted and explaining the services we are making available.

What Information Was Involved? The personal information contained within the impacted data included first and last name, Social Security number, financial account information, including financial account number and/or routing number, credit and/or debit card number, security code, expiration date, and pin, passport number, driver's license or ID number, username and password, date of birth, medical information, and/or health insurance information. The types of impacted information varied by individual and not every data element was impacted for each individual.

What We Are Doing. The security and privacy of the information contained within our systems is a top priority for us. In response to this incident, we took immediate steps to secure our systems and engaged third-party forensic experts to assist in the investigation. Further, we are implementing additional cybersecurity safeguards, as needed, enhancing our employee cybersecurity training, and improving our cybersecurity policies, procedures, and protocols to help minimize the likelihood of this type of incident occurring again.

How Will Individuals Know If They Are Affected By This Incident? We are providing notice to individuals whose information was determined to be contained in the impacted data in accordance with our legal obligations and to the extent we have valid mailing addresses. If an individual does not receive a letter but would like to know if they are potentially affected, they may call (844) 959-7105.

For More Information. We have established a toll-free call center to support our community with any further questions regarding this incident, please call our dedicated assistance line at (844) 959-7105, Monday through Friday, 9 am to 6:30 pm Eastern Time, excluding holidays.

What You Can Do. We encourage individuals to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits forms, and monitoring your free credit reports for suspicious activity and to detect errors. Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report, place a fraud alert, or a security freeze. Contact information for the credit bureaus is below:

Placing a Fraud Alert on Your Credit File.

You may place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(888) 298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze
(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in any credit monitoring service, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600

Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.