CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

Kathleen Monaghan
KMonaghan@c-wlaw.com

Mushu Huang
Mhuang@c-wlaw.com

Three Valley Square, Suite 305
512 E. Township Line Road
Blue Bell, PA 19422

Phone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

July 8, 2026

Via Email: databreach@ag.iowa.gov
Consumer Protection Division
Attorney General of Iowa
Hoover Building
1305 E Walnut Street
Des Moines, IA 50319

RE: Notice of Data Security Event

To Whom It May Concern:

We serve as counsel for Northwest Iowa Community College ("NICC") located at 603 W Park St, Sheldon, IA 51201, and write to inform you of a data security event. By providing this notice, NICC does not waive any rights or defenses under Iowa law, including the data breach notification statute.

On or around November 26, 2025, Northwest Iowa Community College ("NICC") became aware of certain unauthorized activity within its computer systems. Upon discovery, NICC quickly took steps to secure its network and engaged third-party specialists in order to determine the nature and scope of the event. The investigation determined that a limited amount of information may have been accessed or downloaded without authorization between November 24 and November 26, 2025. After the scope of the unauthorized activity was confirmed, NICC then conducted a review of the potentially impacted information to determine the types of information present and to whom the information related. That comprehensive and time-consuming review process was completed on May 29, 2026.

NICC then worked to confirm the up-to-date contact information to provide notice. This process included performing a National Change of Address (NCOA) search to ensure as up-to-date information as possible. On July 6, 2026, NICC received its results from the NCOA search and confirmed that this event potentially affected sixteen thousand four (16,004) Iowa residents. The types of information potentially impacted included the individual's name in combination with their Social Security number.

On July 8, 2026, NICC began mailing written notice to the potentially affected individuals. In an abundance of caution, NICC is offering all individuals complimentary credit monitoring and identity protection services. A representative copy of the notification letter sent to potentially impacted individuals is attached as ***Exhibit A***.

In response to this event, NICC quickly took remediation steps and conducted a forensic investigation, as well as reviewed and enhanced its data security policies and procedures related to data security and cybersecurity. Moreover, NICC notified relevant individuals with an offering of complimentary access to credit monitoring services and a dedicated call center.

If you have any questions, please contact me.

Very truly yours,

Kathleen Monaghan

Kathleen Monaghan, Esquire
CIPRIANI & WERNER, P.C.

Exhibit A

Northwest Iowa Community College
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

NORTHWEST

[redacted]

[redacted]

July 8, 2026

Dear [redacted],

Northwest Iowa Community College ("NICC") writes to notify you of a recent event that may have involved your information as described below. We take the privacy and security of all information seriously, and this letter includes information about the event, our response, and recources we are making available to you.

<u>What Happened</u>:

On or around November 26, 2025, NICC became aware of certain unauthorized activity within its computer systems. Upon discovery, NICC promptly took steps to secure its network and engaged third-party specialists in order to determine the nature and scope of the event. The investigation determined that a limited amount of information may have been accessed or downloaded without authorization between November 24, 2025 and November 26, 2025. After the scope of the unauthorized activity was confirmed, NICC then conducted a review of the potentially impacted information to determine the types of information present and to whom the information related. The comprehensive and time-consuming review was completed on May 29, 2026, after which NICC worked to align resources in order to provide you with this notice.

At this time, we are providing this notification to you out of an abundance of caution and so that you may take steps to safeguard your information if you feel it is necessary to do so.

<u>What Information Was Involved</u>:

The types of information that may have been contained within the affected data include your first and last name, in combination with Social Security number.

<u>What We Are Doing</u>:

NICC has taken steps to address the event and is committed to protecting information in its care. In response to this event, NICC conducted a full investigation aided by third-party forensic specialists into the activity to determine all relevant information. Once the information that may have been impacted was confirmed, NICC diligently reviewed the information and to whom it related in order to assess potential notification obligations. As an additional safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service for 12 months provided by Cyberscout, a TransUnion company. Due to privacy laws, we cannot register you directly. Additional information regarding how to enroll in the complimentary credit monitoring service is enclosed.

What You Can Do:

In addition to enrolling in the complimentary credit monitoring service detailed within, we recommend that you remain vigilant in regularly reviewing and monitoring all your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on any of your accounts, please promptly change your password and take additional steps to protect your account and notify your financial institution or company if applicable. Additionally, please report any suspicious incidents to local law enforcement and/or your State Attorney General. We have provided additional information below regarding how you may protect against fraud and identity theft should you feel it appropriate to do so.

For More Information:

Should you have additional questions or concerns regarding this matter, please do not hesitate to contact our dedicated call center at [redacted], Monday to Friday between the hours of 8:00 a.m. and 8:00 p.m. Eastern Time, excluding holidays. You can also write us at 603 W Park St, Sheldon, IA 51201.

Sincerely,

Northwest Iowa Community College

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Credit Monitoring / Identity Protection

In response to the event, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted] In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com	Experian 1-888-397-3742 www.experian.com	Equifax 1-888-298-0045 www.equifax.com
TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000	**Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013	**Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069
TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	**Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this event.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington, D.C. 20001; 202-442-9828, and https://oag.dc.gov/consumer-protection.