GREGORY N. BRESCIA
GBRESCIA@GRSM.COM

GORDON&REES
SCULLY MANSUKHANI
YOUR 50 STATE PARTNER™

ATTORNEYS AT LAW
500 MAMARONECK AVE, SUITE 503
HARISSON, NY 10528
WWW.GRSM.COM

May 22, 2026

VIA EMAIL (consumer_protection@ag.idaho.gov)
Attorney General's Office
Consumer Protection Division
P.O. Box 83720
Boise, ID 83720-0010

Re: Notification of Data Security Incident
Our File No: 1444481

To Whom It May Concern:

Our client, Cowley County Community College ("Cowley"), a public community college, understands the importance of protecting personal information and is making this notification to your Office in accordance with applicable law following a recent data security incident.

On March 28, 2026, Cowley became aware of a data security incident that impacted its server infrastructure and took its systems offline. Cowley immediately undertook efforts to restore its servers and undertook additional affirmative steps to safeguard the security of data maintained on its systems. Cowley also simultaneously retained a forensic investigation firm to determine the nature of the security compromise and identify any individuals whose information may have been compromised.

The forensic investigation remains ongoing. As of the date of this notification, Cowley is unable to confirm with a reasonable degree of certainly the date on which access to Cowley's systems occurred. The investigation identified certain files that may have been accessed or acquired in connection with the incident. In continuing its thorough investigation, Cowley undertook a comprehensive manual review process to review these files and identify the specific individuals with person information contained therein. This comprehensive manual review process concluded on or about May 1, 2026.

On or about May 8, 2026, the external forensic investigation firm confirmed that the data security involved the unauthorized access to Cowley's system. The forensic investigation confirmed that, during this brief period of unauthorized access, there was unauthorized access to and/or acquisition of certain files maintained on Cowley's system. As a result, Cowley undertook a comprehensive and time intensive review of all files that may have been accessed and/or acquired in connection with the incident to determine the presence of any PII contained therein. As noted above, this comprehensive review process was completed on or about May 1, 2026, at which point

Cowley determined the existence of PII within the files that may have been accessed and/or acquired in connection with the incident.

As stated above, following the data security incident, Cowley immediately undertook all efforts to restore its servers, and also undertook additional affirmative steps to safeguard the security of data maintained on its systems. Cowley retained a forensic investigation firm to thoroughly investigate the incident and providing notification to all individuals whose personal information may have been accessed and/or acquired in connection with the incident in an abundance of caution. Cowley has obtained confirmation to the best of its ability that the information is no longer in possession of the third party(ies) associated with this incident, and it is entirely possible that any specific personal *was not compromised* as a result of the incident. Nonetheless, Cowley has also offered to the impacted individuals access to complimentary credit monitoring. Please be advised that we are continuing to work closely with leading security experts to identify and implement measures to further strengthen the security of Cowley's systems to help prevent this from happening in the future.

Cowley began mailing notification letters on May 22, 2026 to all individuals who's personal may have been accessed and/or acquired in connection with the incident. Of these individuals, we are of the belief that eighteen (18) individuals are Idaho residents. We anticipate that it will take five days for individuals to receive this letter. If an individual does not receive a letter, but would like to know if he or she was potentially affected by this incident, or if an individual has any questions or would like additional information, they may call Cowley's dedicated assistance line at 866-561-6068 between the hours of 9:00am to 5:00pm EST, Monday through Friday.

Should you have any questions or wish to further discuss, please do not hesitate to contact the undersigned.

Sincerely,

Gregory N. Brescia

Cowley County Community College
Return Mail Processing Center
PO Box 173071 | Milwaukee, WI 53217

<<First Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF SECURITY <<HEADER>>

Dear <<First Name>> <<Last Name>>:

Cowley County Community College ("Cowley") writes to inform you of a security incident that may affect the security of some of your information. Although we have received no indication of identity theft or fraud as a result of this event, this notice provides information about the event, our response, and steps you can take to help protect your information from possible misuse.

What Happened? On March 28, 2026, Cowley became aware of suspicious activity in our computer environment. We shut down our server and immediately undertook efforts to safeguard the security of data maintained on our system. We promptly launched an investigation with the assistance of third-party cybersecurity specialists to determine the nature and scope of the incident. The investigation determined that an unauthorized actor gained access to certain systems and accessed and/or acquired certain information contained in those systems. Accordingly, we undertook a comprehensive manual review to determine what type of personal information was on those systems and which individuals were impacted. We then worked to validate the results and locate appropriate contact information for those affected. We recently completed this process and have moved quickly to provide notice to you and all others affected.

What Information Was Involved? The forensic investigation determined that information related to you included one or more of the following: names; contact information; addresses; social security numbers; student identification numbers; driver's license numbers; and passport numbers.

What We Are Doing. We take the security of information seriously. Following the security incident, Cowley immediately undertook efforts to restore our server, assess the security of our system, and retain cybersecurity specialists to safeguard the security of data maintained on our systems. We retained an expert forensic investigation firm to thoroughly investigate the incident, and now we are notifying affected individuals, including you, so that you may take steps to protect your information, should you feel it is appropriate to do so. We regret any inconvenience or concern this event may cause. As an added precaution, we are offering services through Iris Identity Monitoring at no cost to you.

We are continuing to work closely with leading security experts to identify and implement measures to further strengthen the security of our systems to help prevent this from happening in the future.

FREE IDENTITY MONITORING SERVCIES: Additionally, we are providing you with access to Iris Identity Protection at no charge for <<CM Duration>> months. Please visit **https://iris-pro.myidentityprotectiononline.com** and enter the following promo code to enroll and begin your membership: <<Monitoring Code>> (case sensitive). Please note the deadline to enroll is 90 days from the date of this letter. Iris Identity Monitoring provides One-bureau

credit monitoring from Equifax®, Identity Monitoring, Identity Fraud Insurance[1], and Identity Resolution Services.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and credit reports for suspicious activity and to detect errors. Any suspicious activity should be promptly reported to your bank, credit card company, or other applicable institutions. We encourage you to protect yourself from potential harm by closely monitoring all mail, email, or other contact from individuals not known to you personally, and by avoiding answering questions or providing additional information to such unknown individuals. Additional information and resources may be found in the enclosed *Steps You Can Take to Help Protect Your Personal Information*. You may also enroll in the complimentary credit monitoring and identity restoration services available to you. Enrollment instructions are attached to this letter.

For More Information. For further information on steps you can take to prevent against possible fraud or identity theft, please see the enclosed *Steps You Can Take to Help Protect Your Personal Information*. If you have any questions about this incident that are not addressed in this letter, you may contact our dedicated assistance line at 866-561-6086 between the hours of 9:00 a.m. and 5:00 p.m. Eastern Time, Monday through Friday (excluding U.S. holidays). Please have this letter with you if you call.

Sincerely,

Holly Harper

Cowley County Community College

[1] The Identity Expense Reimbursement and the Unauthorized Electronic Fund Transfer Reimbursement benefits are underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Generali Global Assistance, Inc., dba Iris® Powered by Generali for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions. Review the Summary of Benefits at https://www.irisidentityprotection.com/terms-conditions.

Attachment 1: Protecting Yourself

We remind you to remain vigilant for incidents of fraud or identity theft by reviewing account statements and credit reports for unauthorized activity. **Residents of the United States are entitled to one free credit report annually from each of the three major credit reporting agencies.** To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

You may want to consider placing a fraud alert on your credit report. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud – an initial alert and an extended alert.

- **Initial Alert:** You may ask that an initial alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. A fraud alert does not impact your ability to get a loan or credit, but rather alerts a business that your personal information may have been compromised and requires the business to verify your identity before issuing you credit. Although this may cause some delay if you are applying for credit, it may protect against someone else obtaining credit in your name. An initial fraud alert stays on your credit report for at least 90 days
- **Extended Alert:** You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies. The agency that you contacted must notify the other two agencies.

Additionally, you have the right to put a **credit freeze**, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze. However, unlike a fraud alert, you must separately place a security freeze on your credit file at each of the three national credit reporting agencies. In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Below are the toll-free numbers and addresses for the three largest credit reporting agencies:

Equifax
P.O. Box 74021
Atlanta, GA 30374
1-800-685-1111
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Below is the toll-free number, address and website address for the Federal Trade Commission, which you may contact to obtain further information on how to protect yourself from 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

For residents of District of Columbia, Maryland, Rhode Island, and North Carolina: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

Rhode Island Office of the Attorney General
Consumer Protection
150 South Main Street
Providence, RI 02903
1-401-274-4400
www.riag.ri.gov

District of Columbia Office of the Attorney General
Office of Consumer Protection
400 6th Street, NW
Washington, DC 20001
1-202-442-9828
www.oag.dc.gov

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

For residents of Massachusetts and Rhode Island: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

FAIR CREDIT REPORTING ACT. You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list includes the following FCRA rights: (1) To receive a copy of your credit report, which must contain all the information in your file at the time of your request; (2) To receive a free copy of your credit report, at your request, once every 12 months from each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion; (3) To receive a free credit report if a company takes adverse action against you (e.g. denying your application for credit, insurance, or employment), and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft; (4) To ask for a credit score; (5) To dispute incomplete or inaccurate information; (6) To obtain corrections to your report or delete inaccurate, incomplete, or unverifiable information; (7) Consumer reporting agencies may not report outdated negative information; (8) To restrict access to your file and to require consent from you for reports to be provided to employer; (9) To limit "prescreened" offers of credit and insurance you receive based on information in your credit report; and (10) To seek damages from violators. Note - Identity theft victims and active duty military personnel have additional rights.