McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins, LLC
300 North LaSalle Street
Suite 1400
Chicago, IL 60654

P 1.312.280.0111
F 1.312.280.8232

Blair L. Dawson, JD, MS CyS, FIP, CIPP/US, CIPP/E, CIPM
Direct Dial: 312-642-6131
E-mail: bdawson@mcdonaldhopkins.com

January 20, 2026

VIA EMAIL (*consumer@ag.iowa.gov*)
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319-0106

Re: Interstate 35 Community School District – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Interstate 35 Community School District ("Interstate 35 CSD"). I am writing to provide notification of an incident at Interstate 35 CSD that may affect the security of personal information of approximately nine hundred and ten (910) Iowa residents. By providing this notice, Interstate 35 CSD does not waive any rights or defenses regarding the applicability of Iowa law or personal jurisdiction.

On or about March 7, 2025, Interstate 35 CSD experienced a data security incident, where an unauthorized party accessed certain systems in its network environment. Upon learning of this issue, Interstate 35 CSD immediately commenced a prompt and thorough investigation. As part of our investigation, Interstate 35 CSD has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. The investigation determined that certain data on Interstate 35 CSD systems may have been accessed or acquired by an unauthorized party. After an extensive forensic investigation and internal review of the at-risk data, on December 12, 2025, Interstate 35 CSD discovered individual personal information may have been subject to unauthorized access or acquisition. The potentially impacted information includes: Full Name, Driver's License or State ID, Medical Information, and Social Security number.

To date, Interstate 35 CSD is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident. Nevertheless, out of an abundance of caution, Interstate 35 CSD wanted to inform you (and the affected residents) of the incident and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Interstate 35 CSD is providing the affected residents with written notification of this incident commencing on or about January 20, 2026, in substantially the same form as the letter attached hereto. Interstate 35 CSD is offering the affected residents whose Social Security numbers were impacted complimentary memberships with a credit monitoring service. Interstate 35 CSD is advising the affected residents about the process for placing fraud alerts and/or security freezes on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

At Interstate 35 CSD School District, protecting the privacy of personal information is a top priority. Interstate 35 CSD is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Interstate 35 CSD continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (312) 642–6131 or email me at bdawson@mcdonaldhopkins.com.

Sincerely Yours,

Blair L. Dawson, JD, MS CyS, FIP, CIPP/US, CIPP/E, CIPM

Encl.

#ROADRUNNERPRIDE
INTERSTATE 35
COMMUNITY SCHOOL DISTRICT

Secure Processing Center
[redacted]

[redacted]

[redacted]

Dear [redacted]

The privacy and security of the personal information we maintain is of the utmost importance to Interstate 35 Community School District ("Interstate 35 CSD"). We are writing with important information regarding a data security incident. As such, we want to provide you with information about the incident, tell you about the services that we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On or about March 7, 2025, we learned that an unauthorized individual may have gained access to an employee email account.

What We Are Doing

Upon learning of this issue, we immediately commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. The investigation determined certain data on our systems may have been accessed or acquired by an unauthorized party. After an extensive forensic investigation and comprehensive document review, on December 12, 2025, we determined your personal data may have been subject to unauthorized access.

What Information Was Involved?

The information potentially impacted includes your full name and the following [redacted]

What You Can Do

While we have no evidence of financial fraud or identity theft related to this data, we want to make you aware of the incident. Out of an abundance of caution, to help protect your identity, we are offering complimentary identity theft protection services through Epiq Privacy Solutions ID. Epiq's identity protection services include: [redacted] months credit monitoring, a $1,000,000 identity theft insurance, and social security number monitoring. We encourage you to contact Epiq with any questions and to enroll in free identity protection services by going to www.privacysolutionsid.com and using the Activation Code provided below. Please note the deadline for enrolling is [redacted]

This letter provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information

Interstate 35 CSD is committed to maintaining the privacy of personal information in our possession and has taken many precautions to safeguard it. Interstate 35 CSD continually evaluates and modifies its practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted] This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against potential misuse of your information. The response line is available Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, excluding major U.S. holidays.

Sincerely,
Interstate 35 Community School District
405 E North St
Truro, IA 50257

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary [redacted] Month Credit Monitoring.

Please enroll online.

Activation Code: [redacted]
Deadline: [redacted]

Website and Enrollment.

1. Visit www.privacysolutionsid.com and click "Activate Account"
2. Enter the following activation code, [redacted] and complete the enrollment form
3. Complete the identity verification process
4. You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
5. Enter your log-in credentials
6. You will be directed to your dashboard and activation is complete!

Epiq - Privacy Solutions ID enrollments will include one-year enrollments into the following service components:

1-Bureau Credit Monitoring with Alerts - Monitors your credit file(s) for key changes, with alerts such as credit inquiries, new accounts, and public records.

VantageScore® 3.0 Credit Score and Report - 1-Bureau VantageScore® 3.0 (annual) and 1-Bureau Credit Report.

SSN Monitoring (High Risk Transaction Monitoring, Real-Time Authentication Alerts, Real-Time Inquiry Alerts) - Detect and prevent common identity theft events outside of what is on your credit report. Real-time monitoring of SSNs across situations like loan applications, employment and healthcare records, tax filings, online document signings and payment platforms, with alerts.

Dark Web Monitoring - Scans millions of servers, online chat rooms, message boards, and websites across all sides of the web to detect fraudulent use of your personal information, with alerts.

Change of Address Monitoring - Monitors the National Change of Address (NCOA) database and the U.S. Postal Service records to catch unauthorized changes to users' current or past addresses.

Credit Protection - 3-Bureau credit security freeze assistance with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

Personal Info Protection - Helps users find their exposed personal information on the surface web—specifically on people search sites and data brokers – so that the user can opt out/remove it. Helps protect members from ID theft, robo calls, stalkers, and other privacy risks.

Identity Restoration & Lost Wallet Assistance - Dedicated ID restoration specialists who assist with ID theft recovery and assist with canceling and reissuing credit and ID cards.

Up to $1M Identity Theft Insurance - Provides up to $1,000,000 ($0 deductible) Identity Theft Event Expense Reimbursement Insurance on a discovery basis. This insurance aids in the recovery of a stolen identity by helping to cover expenses normally associated with identity theft.

Unauthorized Electronic Funds Transfer - Provides up to $1,000,000 ($0 deductible) Unauthorized Electronic Funds Transfer Reimbursement. This aids in the recovery of stolen funds resulting from fraudulent activity (occurrence based).

2. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one (1) 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

3. 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 you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, 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.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

****

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.