Gregory Lederman
Office: (267) 930-4637
Fax: (267) 930-4771
Email: glederman@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

August 3, 2026

VIA E-MAIL

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

Re: Notice of Data Event

To Whom It May Concern:

We represent PDCM Insurance ("PDCM"), located at 3022 Airport Blvd, Waterloo, IA 50703, and are writing to notify your Office of an incident that may affect the security of information relating to certain Iowa residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, PDCM does not waive any rights or defenses regarding the applicability of Iowa law, the applicability of the Iowa data event notification statute, or personal jurisdiction.

Nature of the Data Event

On April 28, 2025, PDCM became aware of suspicious network activity involving certain computer systems. Upon learning of this activity, PDCM promptly took steps to secure its network, notified law enforcement, and began an investigation to determine the nature and scope of the activity. The investigation determined there was unauthorized access to certain files and folders within the PDCM network between April 27, 2025 and April 28, 2025. As a result, PDCM began an extensive review of the contents of the involved systems to determine whether they contain protected information. This review recently concluded and determined that the information on the involved systems includes name, Social Security number, driver's license number and financial account information. PDCM is notifying relevant data owner clients and individuals with whom it maintained a direct relationship of this incident.

Notice to Iowa Residents

On or about August 3, 2026, PDCM provided written notice of this incident to four thousand seven hundred and thirty-four (4,734) Iowa residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. PDCM also posted notice of this incident on its website and distributed notice to relevant media outlets. Notification to data owner clients and individuals is ongoing and PDCM may supplement this notification if it is determined that a significant number of additional Iowa residents are notified.

Other Steps Taken and To Be Taken

Upon discovering the event, PDCM moved quickly to investigate and respond to the incident, assess the security of PDCM systems, and identify potentially affected data owner clients and individuals. PDCM is also working to implement additional safeguards and training to its employees. PDCM is providing access to complimentary credit monitoring services for twelve (12) months, through Kroll, to individuals whose Social Security number or similar identifier was potentially affected by this incident.

Additionally, PDCM is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements, explanation of benefits forms, and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

PDCM is also providing written notice of this incident to relevant state and federal regulators, as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4637.

Very truly yours,

Gregory Lederman of
MULLEN COUGHLIN LLC

GCL/lcf
Enclosure

EXHIBIT A

PDCM INSURANCE

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

SCAN TO ENROLL

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

<<b2b_text_1 (Notice of Security Incident / Notice of Data Breach)>>

Dear <<First_name>> <<Last_name>>:

PDCM Insurance ("PDCM") is writing to notify you of an incident that may affect the privacy of some of your information. This letter provides details of the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On April 28, 2025, we became aware of suspicious network activity involving certain computer systems. Upon learning of this activity, we promptly took steps to secure our network, notified law enforcement, and began an investigation to determine the nature and scope of the activity. Our investigation determined there was unauthorized access to certain files and folders within our network between April 27, 2025 and April 28, 2025. As a result, we began an extensive review of the involved systems to determine whether they contain protected information.

What Information Was Involved? The investigation recently determined your information was present on the involved systems. The information that relates to you includes your <<b2b_text_2 (name + Data Elements)>>. At this time, we have no indication that your information was subject to identity theft or fraud as a result of this incident.

What We Are Doing. PDCM treats its responsibility to safeguard information as a priority. Upon discovery, PDCM quickly commenced an investigation to confirm the nature and scope of this incident. This investigation and response included confirming the security of our systems, reviewing the contents of relevant data for sensitive information, and notifying potentially impacted clients and individuals. As part of our ongoing commitment to the privacy of information in our care, we implemented additional security measures and reviewed relevant policies and procedures to reduce the likelihood of a similar future event.

What You Can Do. We encourage you to review the information contained in the *Steps You Can Take to Help Protect Your Information* section below. You can remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits, and monitoring your free credit reports for suspicious activity. Enclosed you will also find more information regarding the complimentary credit monitoring services we are making available to you. Although we are covering the cost of these services, due to privacy restrictions, you will need to complete the enrollment process yourself.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (844) 958-8900 between the hours of 9:00 a.m. and 6:30 p.m. EST, Monday – Friday, excluding major U.S. holidays.

Sincerely,

PDCM Insurance

ELN-27568

Steps You Can Take To Help Protect Your Information

Enroll in Monitoring Services

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for <<ServiceTerminMonths>> months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

*You have until **<<b2b_text_6 (activation deadline)>>** to activate your identity monitoring services.*

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. 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. 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.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, 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, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

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

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov. PDCM is located at 3022 Airport Blvd, Waterloo, IA 50703.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/. PDCM is located at 3022 Airport Blvd, Waterloo, IA 50703.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their 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 consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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.