

PMC Insurance Group
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223



To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code:
<<XXXXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

September 21, 2021

Dear <<First Name>> <<Last Name>>,

PMC Insurance Group (“PMC”) is writing to inform you, as a current or former PMC employee, of a recent event that may impact the privacy of some of your information. While we have no indication of any identity theft or fraud occurring as a result of this incident, we are providing you information about the event, our response, and steps you may take to protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? On or about June 14, 2021, PMC became aware of suspicious activity in our computer network. We immediately took steps to secure our network and minimize any disruption to our operations. We launched an investigation into the nature and scope of the incident with the assistance of industry-leading cybersecurity specialists. Through this investigation, we learned that an unauthorized individual accessed our network intermittently between April 16, 2021 and June 13, 2021, and that files containing certain employee information may have been viewed and/or taken by the unauthorized individual.

What Information Was Involved? The investigation determined that the following types of information related to you could be involved: name, address, Social Security number, driver’s license number, and financial account number used for direct deposit.

What We Are Doing. Upon discovering this incident, we moved quickly to investigate and respond, assess the security of relevant PMC systems, and identify any impacted data. As part of our ongoing commitment to the security of information, we are evaluating opportunities to improve security and to better prevent future events of this kind. While we currently do not have evidence of any identity theft or fraud related to this event, we are offering you access to complimentary credit monitoring services for 24 months through IDX. These services include fraud consultation and identity theft restoration services. If you wish to activate the credit monitoring services, you may follow the instructions included in the *Steps You Can Take to Protect Personal Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, and to review your account statements and credit reports for suspicious activity. You may also review the information contained in the attached *Steps You Can Take to Protect Personal Information*. Please note the deadline to enroll is December 21, 2021.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. Should you have any questions, you may contact us at 1-800-939-4170, which can be reached Monday through Friday from 9:00 AM - 9:00 PM Eastern Time.

Sincerely,

Andrew Shaw
Executive Vice President, Managing Partner

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code <<XXXXXXXX>> or call IDX at 1-800-939-4170. IDX representatives are available Monday through Friday from 9:00 AM – 9:00 PM Eastern Time.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Please note the deadline to enroll is December 21, 2021.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of IDX's ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report 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 security freeze, you will need to provide 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 you are a victim of identity theft.

Should you wish to place a credit freeze, 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/credit-help
1-888-298-0045	1-888-397-3742	1-833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, 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 Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

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.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

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 www.oag.state.md.us. PMC is located at 209 Burlington Road, Suite 109, Bedford, Massachusetts 01730.

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 reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are three (3) Rhode Island residents impacted by this incident.