

PINNACLE™

CLAIMS MANAGEMENT, INC.

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

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

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to inform you of a recent data security incident experienced by Pinnacle Claims Management, Inc. (“PCMI”) that may have involved some of your information. PCMI provides health benefits administration. You are receiving this notice because your current or former employer’s health plan had a relationship with PCMI. At PCMI, we take the privacy and security of your information very seriously. That is why we are writing to provide you with information about this incident, about steps you can take to help protect your personal information, and to offer you complimentary identity monitoring services.

What Happened? On June 26, 2022, PCMI became aware of unusual activity within its digital environment. Upon discovering this activity, PCMI immediately took steps to secure its network. PCMI engaged leading cybersecurity firms to conduct an investigation to determine whether personal information hosted on its network may have been impacted as a result of the incident. The investigation revealed that an unauthorized actor may have acquired certain PCMI data. On September 28, 2022, we determined that some of your personal information may have been involved in this incident. We have no reason to believe that your personal information has been misused as a result of this incident.

What Information Was Involved? The information impacted in connection with this incident may have included your <<b2b_text_2 (“name” and data elements)>>.

What Are We Doing? As soon as PCMI discovered the incident, we took the measures described above and implemented additional security features to reduce the risk of a similar incident occurring the in the future. We are further notifying you of this event and advising you about steps you can take to help protect your information. In addition, out of an abundance of caution, we are offering you complimentary identity monitoring services for 12 months through Kroll, a global leader in risk mitigation and response.

Kroll’s services include 12 months of Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to help protect your information. You can also activate Kroll’s identity monitoring services, which are offered to you at no cost.

How to Activate:

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>>

To receive identity monitoring 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. For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com. Additional information describing your services is included with this letter.

Kroll representatives are available by calling (855) 532-1931 Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please note the deadline to activate is <<b2b_text_6 (activation deadline)>>. Please do not discard this letter, as you will need the Membership Number provided above to access services.

We take your trust in us and this matter very seriously and we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Pinnacle Claims Management, Inc.

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant, especially over the next 12 to 24 months, and review your account statements and credit reports closely. 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 (the “FTC”).

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax	Experian	TransUnion	Free Annual Report
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	www.annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Iowa, Maine, Maryland, North Carolina, Oregon, New York, Rhode Island, Vermont, and Washington D.C. can obtain more information from their Attorneys General using the contact information below.

Iowa: You are advised to report any suspected identity theft to law enforcement or to the Office of the Attorney General of Iowa, 1305 E Walnut St, Des Moines, IA 50319, 1- 888-373-5044, <https://www.iowaattorneygeneral.gov/>.

Maine: Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-626-8800; <https://www.maine.gov/ag/>.

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 1-888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

North Carolina: North Carolina Attorney General’s Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

Oregon: You may also contact the Oregon Office of the Attorney General: Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096, 1-877-877-9392, help@oregonconsumer.gov, www.doj.state.or.us.

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005, 1-212-416-8433, <https://ag.ny.gov/>.

Rhode Island: Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, <http://www.riag.ri.gov>.

Vermont: Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; Phone (802) 828-3171; Email: ago.info@vermont.gov.

Washington D.C.: Washington D.C. Attorney General can be reached at: 441 4th Street, NW Washington, DC 20001, 1-202-727-3400, oag.dc.gov.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

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.