

July 28, 2023

SHOOK
HARDY & BACON

VIA email to idtheft@oag.state.md.us

Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202

Jonathan L. Wilson

1800 K Street NW Suite 1000
Washington, D.C. 20006
t 202.783.8400
dd 202.662.4863
f 202.783.4211
jlwilson@shb.com

RE: Security Incident

Dear Sir/Madam:

I am writing on behalf of Bank of the Rockies to notify you of a security incident involving the personal information of one Maryland resident.

On April 4, 2023, Bank of the Rockies noticed suspicious activity in its email system and immediately took steps to begin investigating the incident and securing its environment. It promptly engaged Shook, Hardy & Bacon as outside counsel, and we, in turn, immediately engaged a leading digital-forensics firm to assist us in the investigation. Based on our investigation, we believe an unknown third party gained access to a limited number of email accounts from March 30, 2023 to April 4, 2023. Once we identified the files within those email accounts that may have been affected, we immediately engaged a data-review firm to determine what personal information, if any, was in those files. We received the results of that review on June 28, 2023. Since then, we have been diligently working with Bank of the Rockies to identify the correct addresses for the affected individuals and assess notification obligations.

Having reviewed the data, we now have reason to believe that the unknown third party potentially accessed the personal information of one Maryland resident. The unknown third party may have accessed files containing some combination of the following: full names, contact information, government identification (such as a driver's license or Social Security number), and financial information (such as a bank account number but not any security or access code related to that account). At this time, we have no reason to believe the information was, or will be, misused.

Bank of the Rockies will begin notifying the potentially affected individuals on July 28, 2023, and enclosed is a sample of the notification letter. In the letter, Bank of the Rockies provides each individual with one year of Experian IdentityWorks, a credit-monitoring service, and a toll-free call center has been set up to field any questions individuals have about the incident.

In addition to providing notice, Bank of the Rockies has taken a variety of measures to bolster its security. For example, Bank of the Rockies changed passwords, adopted new technical safeguards, and provided additional phishing training to employees. Bank of the Rockies also notified law enforcement.

Please contact me if you have any questions or need any additional information regarding this incident.

Sincerely,



Jonathan Wilson
Senior Counsel



Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

FIRST_NAME LAST_NAME
ADDRESS1
CITY, STATE zip

July 28, 2023

NOTICE OF DATA BREACH

Dear First_Name Last_Name:

At Bank of the Rockies, we take seriously our relationship with you, and for that reason we are reaching out with information on a cyberattack we experienced in late March affecting a portion of our email system. This attack may have exposed some of your personal information. In response, we have taken a variety of measures to bolster our security and are providing you this notice with details about additional steps you can take.

WHAT HAPPENED

On April 4, 2023, we determined that an unauthorized third party gained access to a limited portion of our email system between March 30, 2023, and April 4, 2023. After discovering the incident, we promptly took steps to terminate that access and began working with outside experts to investigate. While that work was underway, we retained a data-review firm to identify individuals whose information may have been in the affected emails. The review firm provided those results on June 28, 2023, and we have worked since then to identify correct addresses for those individuals.

WHAT INFORMATION WAS INVOLVED

Our investigation determined that the following types of information were present in the email accounts at issue: full name, contact information, government identification (such as Social Security or driver's license number), and financial information (such as your bank account number but not any security or access code related to that account). But, importantly, we do not have confirmation that the third party actually viewed/downloaded the emails containing that data or that the affected information will be (or has been) misused.

WHAT WE ARE DOING

We hired third-party experts to address this situation, perform an investigation into the unauthorized activity, and further secure our systems to protect your information – including changing passwords and blocking IP addresses associated with the attack. We also notified law enforcement, which did not delay this notice.

WHAT YOU CAN DO

Unfortunately, in today's world cyber incidents are a regrettably common occurrence despite precautions. As we continue to further enhance our network security, we encourage you to also take action to protect your information. On the next page, we are providing information on steps you can take – including instructions for activating your free credit monitoring.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at (866) 982-4514, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

A handwritten signature in dark ink, appearing to read "Michael E. Grove". The signature is fluid and cursive, with a large "M" and "G".

Michael E. Grove
President CEO
Bank of the Rockies
2000 Prospect Avenue
Helena, MT 59601

ROCK-ADT

ADDITIONAL STEPS YOU CAN TAKE

Activate your complimentary credit monitoring – To help protect you from fraud or identity theft, we are offering a complimentary one-year membership to Experian's IdentityWorks. This product helps detect possible misuse of your personal information. To register, please:

- Ensure that you **enroll by: date** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- Provide your **activation code: code**

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at (877) 288-8057 by **date** and provide them with the engagement number **engagement code**.

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.IdentityTheft.gov.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which will prevent them from extending you credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

TransUnion
P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

Equifax
P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222

Maryland Attorney General
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

You can also find your Attorney General's contact information at: <https://www.usa.gov/state-attorney-general>.

