R·Y·B·D
ADVISORS & ACCOUNTANTS

[redacted]

[redacted]

Enrollment Code: [redacted]
Enrollment Deadline: [redacted]
To Enroll, Scan the QR Code Below:

[redacted]

SCAN ME
Or Visit:
[redacted]

June 26, 2026

[redacted]

Dear [redacted]:

The privacy and security of the personal information we maintain is of the utmost importance to Rhodes, Young, Black, and Duncan (“RYBD”). RYBD provides tax and accounting services to businesses, including [redacted]. We are writing to provide you with information regarding a recent cybersecurity incident that potentially involved your personal information provided to us by [redacted]. Please read this notice carefully, as it provides information about the incident, the complimentary identity monitoring services we are making available to you, and precautionary measures you can take to protect your information.

On October 12, 2025, RYBD detected unauthorized access to one of our backup servers. We immediately activated our incident response plan and launched an investigation with the assistance of outside cybersecurity and legal professionals to contain the environment and determine root cause and impact on any data.

Our investigation determined the unauthorized parties accessed our network on September 17, 2025 and exfiltrated data before we detected the unauthorized access. We have been working diligently with outside consultants to ensure that all parties involved are identified. On or about May 27, 2026, [redacted] was notified that your personal information may have been accessed or acquired by the unauthorized party. The information that may have been compromised contained [redacted].

To date, we do not have evidence that your information has been used to commit financial fraud or identity theft. Nevertheless, out of an abundance of caution, we want to make you aware of the incident and provide complimentary credit monitoring services as a precaution. We are providing you with access to [redacted] months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services.

This letter also provides information about precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and 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.

If you have questions, please contact our dedicated and confidential call center at [redacted]**.** [redacted]. We apologize for any inconvenience or concern this may cause. We have taken this matter very seriously and will continue to take significant measures to protect the personal information in our possession.

Sincerely,

Rhodes, Young, Black, and Duncan
2055 Sugarloaf Circle, Suite 200
Duluth, GA 30097

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary Credit Monitoring.

1. **Website and Enrollment.** Scan the QR image or go to [redacted] and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the deadline to enroll is [redacted].

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 [redacted] to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

2. Placing a Fraud Alert.

We recommend that you place a one-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
Equifax Information Services LLC
P.O. Box 105069, Atlanta, GA 30348-5069
www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
1-888-EQUIFAX (1-888-378-4329)

Experian
P.O. Box 9532, Allen, TX 75013
www.experian.com/fraud
1-888-EXPERIAN
(1-888-397-3742)

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000, Chester, PA 19016
www.transunion.com/fraud-alerts
800-916-8800; 800-680-7289

3. Consider 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 cost. 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 sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
Equifax Information Services LLC
P.O. Box 105788, Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
1-888-EQUIFAX (1-888-378-4329)

Experian Security Freeze
P.O. Box 9554, Allen, TX 75013
www.experian.com/freeze
1-888-EXPERIAN
(1-888-397-3742)

TransUnion Security Freeze
P.O. Box 160, Woodlyn, PA 19094
www.transunion.com/credit-freeze
800-916-8800; 888-909-8872

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information such as copy of a government issued identification. 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 a credit monitoring service, 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. Protecting Your Medical Information.

If this notice letter indicates that your medical information was impacted, we have no information to date indicating that your medical information involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from medical identity theft.

Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.

Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.

Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

6. 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.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.