6001 E. Front Street
Kansas City, MO 64120

March 21, 2023

000001

[redacted]

RE: Notice of Data Breach

We are writing to inform you of a cybersecurity incident recently discovered by Black & McDonald and the potential implications for your personal information as a result of that incident. We also want to advise you of the steps we've taken since discovering the incident, as well as some which you can take to address the concerns you may have regarding this incident.

What Happened

On February 9, 2023, we detected unusual activity on our network which generated an alert on our network security software. We immediately initiated an investigation and determined that an unauthorized third party gained access to our network. Based on our investigation, we believe they had access from February 8, 2023, to February 9, 2023. Further investigation revealed that a number of our systems were either fully encrypted or in the process of being encrypted. We have reason to believe that personal information pertaining to certain Black & McDonald employees was compromised in relation to this incident. Unfortunately, we do not have specifics as to what information was affected for each individual. Thus, we are notifying you out of an abundance of caution and so that you can take steps to protect yourself should you wish to do so.

What Information Was Involved

As a former employee of Black & McDonald, our investigation indicates that the following types of personal information related to you may have been impacted: name, birthdate, home address, email address, phone number, bank direct deposit information, salary, driver's license, Social Security number and other employment-related information.

What We Are Doing

We have security measures in place that allow us to take prompt action against attempted intrusions into our network. Those measures were implemented here and reduced the scope of the third party's activity. 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. We notified law enforcement, and this notice was not delayed by a law enforcement investigation.

What You Can Do

Activate your complimentary credit monitoring – To guard against any potential misuse of your information, we are offering you 24 months of credit monitoring services through Cyberscout, a TransUnion company specializing in fraud assistance and remediation services on a fully complimentary basis. This credit monitoring service will notify you by email of critical changes to your Credit Report. Should you receive an email alert, you can review and validate the reported change by logging into the portal. This allows you to identify any potentially fraudulent activity on your Credit Report.

We encourage you to take advantage of this service and help protect your identity. To activate your service, please visit:

[redacted]

You will be prompted to enter the following activation code:

[redacted]

Please ensure that you redeem your activation code before 6/30/2023 to take advantage of the service.

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/DataBreach.

- 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. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. 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.

Federal Trade Commission	**Equifax**	**Experian**	**TransUnion**
600 Pennsylvania Ave. NW	P.O. Box 740241	P.O. Box 9701	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(202) 326-2222	(800) 685-1111	(888) 397-3742	(888) 909-8872
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com

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

For New York Residents: the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224; 1-800-771-7755; **https://ag.ny.gov/**.

For More Information

Protecting the privacy of your personal information is important to us, and we regret any inconvenience this incident may cause you. Please know that we are doing everything that we can to assist and guide you through this process. Should you have any questions or concerns, you can contact us at [redacted] between the hours of 8:00 a.m. and 8:00 p.m. EST Monday to Friday, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

DLeiba

Denisa Leiba
Vice President, Human Resources
Black & McDonald