EXHIBIT A

CPAS / ADVISORS

blue

<<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 (NOTICE OF SECURITY INCIDENT/NOTICE OF DATA BREACH)>>

Dear <<First_Name>> <<Last_Name>>:

Blue & Co., LLC ("Blue" or "We") writes to inform you of an incident that may affect some of your information. This letter provides details of the incident, our response, and resources available to help protect your information should you feel it is appropriate to do so.

What Happened? On December 9, 2024, Blue learned of an unauthorized actor who claimed to have taken data from one server in Blue's IT environment. After identifying this matter, Blue quickly isolated the impacted server and launched an investigation with the assistance of third-party forensic specialists. This investigation revealed that there was unauthorized access to an endpoint on or about November 7, 2024, for less than a half-hour, at which time data was removed. Blue then engaged third-party data review specialists to perform a detailed review of the data involved to understand the contents of that data, whether it was sensitive, and to whom it relates. This review was completed on May 20, 2025. Blue was able to identify that information provided to Blue by certain companies was impacted. Blue worked to gather address information for impacted individuals, and on June 23, 2025, Blue determined information related to you could be affected.

What Information Was Involved? The information that could have been impacted by this event includes your name and the following: <<b2b_text_2 (Data Elements)>>.

What We Are Doing. We take the security of information in our care very seriously. Upon learning of the incident, we moved quickly to investigate and notify our business partners and potentially affected individuals. We also reported the event to law enforcement and implemented additional safeguards related to data privacy and security.

In an abundance of caution, we are offering you access to identity monitoring services for <<ServiceTermninMonths>> months through Kroll at no cost to you. The deadline to activate these services is <<b2b_text_6 (Activation Deadline)>>. A description of services and instructions on how to activate can be found within the enclosed *Steps You Can Take to Help Protect Your Information*. Please note that you must complete the activation process yourself as we are not permitted to activate these services for you.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits, and monitoring your free credit reports for suspicious activity and to detect errors over the next 12 to 24 months. You can also review the enclosed *Steps You Can Take to Help Protect Your Information* which contains guidance regarding what you can do to better protect against possible misuse of your information.

For More Information. We understand you may have questions that are not addressed in this letter. If you have questions, please call (866) 819-2990 Monday through Friday between the hours of 9:00 a.m. and 6:30 p.m. Eastern Time, excluding major U.S. holidays. You can write to us at Blue & Co, LLC., 12800 N. Meridian Dr., Suite 400, Carmel, IN 46032.

Sincerely,

Blue & Co., LLC

Steps You Can Take To Protect Personal Information

Activate Monitoring Services

KROLL

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. 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.

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.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (ActivationDeadline)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number (S_N)>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

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 a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any 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 a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of 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 they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
www.equifax.com/personal/credit-report-services/	www.experian.com/help/	www.transunion.com/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, 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, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant 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, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/. You may write to Blue & Co., LLC at 12800 N. Meridian Dr., Suite 400, Carmel, IN 46032.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Massachusetts residents, under Massachusetts law, you have the right to obtain any police report filed 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.

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. You may write to Blue & Co., LLC at 12800 N. Meridian Dr., Suite 400, Carmel, IN 46032.