Jason Cherry, Partner
Cybersecurity & Data Privacy Team
2029 Century Park East
Suite 1100
Los Angeles, CA 90067
jcherry@consatngy.com
Direct: 207.745.1397

March 5, 2025

VIA ELECTRONIC MAIL
Attorney General Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: Idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP, represents Amerman Ginder & Co, LLC ("Amerman") in connection with a recent data security incident described in greater detail below. This notice is being sent because personal information for Maryland residents may have been involved in the incident.

1. Nature of the Security Incident

On September 28, 2024, Amerman became aware of unusual network activity and immediately took steps to secure its systems. Amerman engaged cybersecurity experts to assist with the process. The investigation determined that certain Amerman data may have been acquired without authorization on or around September 28, 2024. After undertaking a review of the potentially affected files, Amerman identified certain personal information that may have been involved. Amerman's review concluded on February 28, 2025 and revealed the individuals whose personal information could have been involved.

2. Number of Maryland Residents Involved

Beginning March 5, 2025, Amerman notified nine (9) Maryland residents of this data security incident via U.S. First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

The personal information involved in this incident includes individuals' names, and Social Security numbers.

3. Steps Taken to Address the Incident

As soon as the Amerman discovered this unusual network activity, it took steps to secure the affected systems and launched an investigation to determine whether, and to what extent, personal information had been accessed or acquired without authorization. Amerman has also implemented additional security measures in an effort to prevent a similar incident from occurring in the future. Further, as referenced in the sample consumer notification letter, the Amerman has offered individuals 12 months of complimentary services through Kroll, which include Credit Monitoring, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Amerman has established a toll-free call center through Kroll to answer questions about the incident and address related concerns.

4. Contact Information

Amerman remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at jcherry@constangy.com.

Sincerely,

Jason Cherry
Partner
Constangy, Brooks, Smith & Prophete, LLP

Enclosure: Sample Notification Letter

Amerman
Ginder&Co.LLC
Certified Public Accountants

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

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

Subject: Notice of Data Security Incident

Dear <<first_name>> <<last_name>>:

We are writing to inform you of a data security incident that may have affected your personal information. At Amerman Ginder & Co, LLC ("Amerman") we take the privacy and security of personal information very seriously. This is why we are informing you of the incident, providing you with steps you can take to help protect your personal information, and offering you complimentary identity monitoring services.

What Happened. On September 28, 2024, Amerman became aware of unusual network activity and immediately took steps to secure our systems. We engaged cybersecurity experts to assist with the process. The investigation determined that certain Amerman data may have been acquired without authorization on or about September 28, 2024. As a result, Amerman engaged additional experts to undertake a review of the potentially affected files. Our review concluded on February 28, 2025, and identified that some of your information may have been involved.

What Information Was Involved. The potentially affected information may have included your name as well as your <<b2b_text_1 (data elements)>>.

What We Are Doing. As soon as Amerman discovered the incident, we took the steps described above and implemented measures to enhance network security and minimize the risk of a similar incident occurring in the future. We also notified the Federal Bureau of Investigation and will provide whatever cooperation may be necessary to hold the perpetrators accountable.

In addition, we have secured the services of Kroll to provide identity monitoring services at no cost to you for <<Monitoring Term Length (Months)>> months. Kroll is a global leader in risk mitigation and response, and the Kroll team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

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>>**

What You Can Do: 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 in the Kroll identity monitoring services, which are offered to you at no cost, using the instructions above. Please note the deadline to activate in these complimentary services is <<b2b_text_6 (activation deadline)>>. Please do not discard this letter, as you will need the Membership Number provided above to access services.

For More Information. If you have questions about this letter or need assistance, please call Kroll at (866) 497-8990. Kroll representatives are available Monday through Friday from 9:00 am – 6:30 pm Eastern Time, excluding major US holidays. Kroll representatives have been fully versed on the incident and can answer questions or concerns you may have regarding safeguarding of your personal information.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience this may cause.

Sincerely,

Amerman Ginder & Co, LLC
205 Narrows Dr,
Lebanon, PA 17046

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing 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 also should 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 (FTC).

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 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.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 at least 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: You have the right to put a security freeze on your credit file for up to one year at no cost. 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 fraud alerts, security freezes, and 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.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

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

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

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.

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.