GT GreenbergTraurig

Kevin M. Scott
Tel 312.456.1040
Fax 312.456.8435
scottkev@gtlaw.com

April 8, 2021

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

attorneygeneral@doj.nh.gov

Re: Notification of Security Incident

Dear Attorney General Formella:

We are writing to inform you that our client, Aero Design & Manufacturing, Inc. ("ADM"), has notified 1 individual who resides in New Hampshire of a data security incident that may have impacted some of their personal information.

ADM was recently the target of a sophisticated ransomware attack. On February 22, 2021, ADM discovered that the attackers accessed its HR folder containing personal information which could include one or more of the following data elements in addition to the individual's name: address, date of birth, Social Security number, direct deposit financial account information, or protected health information associated with health benefit plans enrollment. ADM took immediate action to isolate the attack, investigate, and secure its IT environment. ADM also reported the attack to law enforcement.

ADM takes the security of individuals' information seriously and has taken measures to reduce the likelihood of a future cyber-attack, including increased network security measures and employee training to recognize external attacks.

ADM provided notice to the potentially affected employee on April 7, 2021. A copy of the notification letter is attached. The three major Credit Reporting Agencies are also being notified.

ADM is offering identity theft protection services through Kroll. Services include 12 months of credit monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. Information regarding these services, as well as additional information to assist with enrollment, is included in the notification letter mailed to all potentially affected individuals.

Please contact me for any additional information.

Very Truly Yours,

Kevin M. Scott
Shareholder

KMS:

<<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(SubjectLine)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to notify you of a recent data security incident that may have impacted some of your personal information. We take the security of your information very seriously and sincerely apologize for any concern this incident may cause. This letter contains information about what happened, actions we have taken to prevent a reoccurrence, and steps you can take to help protect your information.

What Happened?
Aero Design & Manufacturing, Inc. was recently the target of a sophisticated ransomware attack. Ransomware is a computer virus that encrypts computer systems, holding those systems hostage with the goal of extorting money to decrypt the systems. We took immediate action to isolate the attack, investigate, and secure our IT environment. We also reported the attack to law enforcement. Our investigation revealed that the personal information of current and former employees and those family members enrolled in our benefits programs or designated as beneficiaries may have been exposed to the attackers.

What information was involved?
On February 22, 2021, we discovered that the attackers accessed our HR folder containing personal information which could include one or more of the following data elements in addition to your name: address, date of birth, Social Security number, direct deposit financial account information, or protected health information associated with health benefit plans enrollment. While we have no evidence that your information was viewed by the attackers, we are notifying you because we cannot conclusively rule out that possibility.

What We Are Doing
We take the security of your information seriously and have taken measures to reduce the likelihood of a future cyber-attack, including increased network security measures and employee training to recognize external attacks. In addition, out of an abundance of caution, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

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

*You have until **July 7, 2021** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

What You Can Do
Please review the enclosed "Additional Important Information" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission (FTC) regarding identity theft protection and details on how to place a fraud alert or security freeze on your credit file. As an added precaution, you may want to closely monitor your personal accounts for any suspicious activity.

For More Information
If you have additional questions or concerns regarding this incident, please call 1-???-???-????, Monday through Friday from 7:00 am – 4:30 pm Mountain Time.

Protecting your information is of the utmost importance to us. We appreciate your patience and understanding, and we sincerely apologize for any inconvenience or concern this incident may cause you.

Sincerely,

Michael Holmes
President

Additional Important Information

For residents of Iowa: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights pursuant to the federal Fair Credit Reporting Act. Please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission listed below.

For residents of District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island:
You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

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

Rhode Island Office of Attorney General
150 South Main Street
Providence RI 02903
1-401-274-4400
www.riag.ri.gov

North Carolina Attorney General
9001 Mail Service Ctr
Raleigh, NC 27699
1-877-566-7226
www.ncdoj.com

New York Attorney General
120 Broadway
3rd Floor
New York, NY 10271
800-771-7755
www.ag.ny.gov

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Ave, NW Washington, DC 20580
1-877-IDTHEFT (438-4338) www.identitytheft.gov

Massachusetts and Rhode Island residents: You have the right to obtain a police report if you are a victim of identity theft.

For residents of all states:
It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for unauthorized activity. You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (https://www.experian.com/fraud/center.html), or Transunion (https://www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze for yourself or your spouse or a minor under 16: (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
https://www.equifax.com/personal/credit-report-services/
800-525-6285

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013-9544
https://www.experian.com/help/
888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19014-0200
https://www.transunion.com/credit-help
800-680-7289

KROLL

Credit Monitoring

We have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services[1] include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Identity Monitoring Services

1. You must activate your identity monitoring services by July 7, 2021. Your Activation Code will not work after this date.
2. Visit **https://enroll.idheadquarters.com** to activate your identity monitoring services.
3. Provide Your Membership Number: **<<Member ID>>**

Take Advantage of Your Identity Monitoring Services

You've been provided with access to the following services[1] from Kroll:

Triple Bureau Credit Monitoring
You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—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 can help you determine if it's 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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1]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.