LEWIS BRISBOIS BISGAARD & SMITH LLP

Kamran Salour
650 Town Center Drive, Suite 1400
Costa Mesa, California 92626
Kamran.Salour@lewisbrisbois.com
Direct: 714.966.3145

November 20, 2020

VIA EMAIL

Attorney General Gordon J. MacDonald
Office of the Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301
Email: attorneygeneral@doj.nh.gov

Re: Notification of Data Security Incident

Dear Attorney General MacDonald:

We represent Universal Automation & Mechanical Services, Inc. ("UAM Services") in connection with a recent data security incident, which is described in greater detail below. UAM Services is a commercial and building management services provider based in Walpole, Massachusetts. UAM Services takes the protection of all sensitive information within its possession very seriously and is taking steps to prevent similar incidents from occurring in the future.

1. **Nature of the security incident.**

UAM Services recently learned of unusual activity involving a UAM Services email account. Upon discovering this activity, UAM Services immediately began an investigation and took steps to secure its email system. UAM Services also engaged an independent, digital forensics firm to determine what happened and whether personal information had been accessed or acquired without authorization. The forensic investigation ultimately concluded that a UAM Services email account may have been accessed without authorization. UAM Services promptly commenced a thorough review of the contents of the identified account to determine whether any personal information may have been contained therein.

On September 29, 2020, UAM Services learned that personal information belonging to five (5) New Hampshire residents was contained within the email account. The information potentially impacted by this incident may have included the notified individual's name, Social Security number, and financial account information

2. Number of New Hampshire Residents Potentially Affected.

UAM Services issued notification letters to the five (5) New Hampshire residents regarding this data security incident via written letter mailed on November 20, 2020. A sample copy of the notification letter is attached hereto.

3. Steps taken relating to the incident.

UAM Services has taken steps in response to this incident to enhance the security of personal information in its possession in an effort to prevent similar incidents from occurring in the future. These measures included: mandating password resets, implementing multi-factor authentication for all user accounts within its environment, as well as enabling unified audit logging features to detect any future suspicious activity within its email environment going forward. In addition, UAM Services requested the assistance of the digital forensics firm to implement a program for regulating and prohibiting the email transmission of any unsecured sensitive or personal information going forward. Furthermore, UAM Services has offered complimentary credit monitoring and identity theft protection services through IDX (formerly ID Experts) to all individuals potentially impacted by this incident, as an added layer of protection.

4. Contact information.

UAM Services remains dedicated to protecting the personal information in its possession. If you have any questions, or need additional information, please do not hesitate to contact me at (714) 966-3145, or by e-mail at Kamran.Salour@lewisbrisbois.com.

Respectfully yours,

Kamran Salour of
LEWIS BRISBOIS BISGAARD & SMITH LLP

KS
cc: Jenna Disser, Lewis Brisbois Bisgaard & Smith

Enclosure: Consumer Notification Letter (Sample)

UNIVERSAL AUTOMATION
& MECHANICAL SERVICES INC.

C/O IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

November 20, 2020

Subject: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

I am writing to inform you of a data security incident that may have affected your personal information. At Universal Automation & Mechanical Services, Inc. ("UAM Services"), we take the privacy and security of personal information very seriously. We are contacting you to notify you that this incident occurred and inform you about steps you can take to ensure your information is protected, including enrolling in the complimentary identity protection services we are making available to you.

What Happened? UAM Services learned of unusual activity involving a UAM Services email account. Upon discovering this activity, we immediately began an investigation and took steps to secure our email system. We also engaged an independent digital forensics firm to determine what happened and whether personal information had been accessed or acquired without authorization. The forensic investigation concluded that a UAM Services email account may have been accessed without authorization on or about July 14, 2020. On September 29, 2020, we learned that some of your personal information was contained within the email account. As soon as we discovered that the incident may have affected personal information, we immediately commenced a diligent search to identify the specific data sets and current mailing addresses for each potentially impacted individual in order to notify them of the incident and provide guidance on steps to take to protect such information.

Please note that this unauthorized access was limited to information transmitted via email and did not affect any other UAM Services information systems. We are not aware of the misuse of any personal information that may have been involved in this incident.

What Information Was Involved? The affected information may have included your name <<variable text>>.

What Are We Doing? As soon as we discovered this incident, we took the steps described above. We have also implemented additional safeguards to help ensure the security of our email environment and to reduce the risk of a similar incident occurring in the future.

In addition, we are providing you with information about steps you can take to help protect your personal information and, as an additional measure, we are offering you 12 months' of credit monitoring and identity theft restoration services at no cost to you through IDX, a leader in risk mitigation and response. These services include credit and CyberScan™ monitoring, a $1,000,000 insurance reimbursement policy, exclusive educational materials, and fully managed identity theft recovery services.

To receive the credit monitoring services offered through IDX, you must be over the age of 18, have established credit in the United States, have a Social Security number issued in your name, and have a United States residential address associated with your credit file. Please note that the deadline to enroll in the complimentary identity protection services is February 20, 2021.

What Can You Do? We recommend that you review the guidance included with this letter about how to help protect your information. We also encourage you to enroll in the complimentary identity protection services offered through IDX by calling 1-800-939-4170 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available to assist you Monday through Friday from 9 am – 9 pm Eastern Standard Time.

We encourage you to take full advantage of this service offering. IDX representatives are fully versed on the incident and can answer any questions you may have about steps you can take to protect your information, as well as the process for enrolling in the complimentary identity protection services.

For More Information: Further information about how to help protect your personal information, as well as detailed instructions for enrolling in the complimentary identity protection services, are enclosed on the subsequent pages of this letter. If you have questions or need assistance with enrollment, please call our dedicated call center at 1-800-939-4170 Monday through Friday from 9 am – 9 pm Eastern Standard Time.

We take your trust in us and the protection of your information very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

Michelle Sullivan, President
Universal Automation & Mechanical Services, Inc.

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

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 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three credit bureaus is as follows:

Equifax Fraud Reporting	**Experian Fraud Reporting**	**TransUnion Fraud Reporting**
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year. **Please Note: No one is allowed to place a fraud alert on your credit report except you.**

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the Federal Trade Commission (contact information below). The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Federal Trade Commission
Identity Theft Clearinghouse
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.consumer.gov/idtheft
1-877-IDTHEFT (438-4338)
TTY: 1-866-653-4261