EXHIBIT 1

By providing this notice, AUI Partners, LLC ("AUI") does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about August 24, 2020, AUI became aware of suspicious activity related to certain employee email accounts. AUI immediately launched an investigation which included working with a third-party forensic investigation firm to determine what may have happened. On September 24, 2020, the investigation confirmed that certain AUI email accounts were accessed by an unknown party. Unfortunately, the investigation was not able to determine which emails, if any, were viewed.

Since AUI was unable to determine what emails were viewed, AUI completed a programmatic and manual review to determine whether sensitive information was present in the emails at the time of the incident. On December 21, 2020, AUI determined personal information was present in one of the relevant email accounts. AUI provided notification out of an abundance of caution because personal information was present in an email account at the time of the incident. AUI then worked to locate address information for the individuals whose personal information may have been contained within the email accounts.

The information that could have been subject to unauthorized access includes name, address, Social Security number and financial account information

Notice to Maine Residents

On or about March 24, 2021, AUI provided written notice of this incident to all affected individuals, which includes two (2) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, AUI moved quickly to investigate and respond to the incident, assess the security of AUI systems, and notify potentially affected individuals. AUI is also working to implement additional safeguards and training to its employees. AUI is providing access to credit monitoring services for twelve (12) months through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, AUI is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud. AUI is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

EXHIBIT A

<<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>>,

AUI Partners, LLC ("AUI") writes to notify you of an incident that may affect the privacy of some of your information. We take this incident seriously, and this letter provides details of the incident, our response, and steps you may take to better protect against possible misuse of your personal information, should you feel it appropriate to do so.

What Happened? On August 24, 2020, AUI became aware of suspicious activity related to certain employee email accounts. We immediately launched an investigation which included working with a third-party forensic investigation firm to determine what may have happened. On September 24, 2020, the investigation confirmed that certain AUI email accounts were accessed by an unknown party. Unfortunately, the investigation was not able to determine which emails, if any, were viewed.

Since we are unable to determine what emails were viewed, we completed a programmatic and manual review to determine whether sensitive information was present in the emails at the time of the incident. On December 21, 2020, we determined your personal information was present in one of the relevant email accounts. We are providing you this notification out of an abundance of caution because your personal information was present in an email account at the time of the incident.

What Information Was Involved? Our investigation determined that the information accessible within the email accounts included your <<b2b_text_2(ImpactedData)>><<b2b_text_3(ImpactedDataCont)>>. Please note that while our investigation did not reveal evidence that your information was actually viewed by the unauthorized actor, we are providing you this notice to ensure you are aware of this incident.

What We Are Doing. Information privacy and security are among our highest priorities. Upon learning of this incident, we quickly took steps to confirm the security of our systems, including our employee email accounts. We reset passwords for all relevant AUI email accounts, implemented multifactor authentication and are reviewing our company policies and procedures relating to data security.

In an abundance of caution, we are notifying potentially affected individuals, including you, so that you may take further steps to help protect your personal information, should you feel it is appropriate to do so. We have arranged to have Kroll provide identity monitoring services for 12 months at no cost to you as an added precaution.

What You Can Do. While we are unaware of misuse of information relating to you, we encourage you to remain vigilant against incidents of identity theft and fraud and to review the information in the attached "*Steps You Can Take to Protect Personal Information*." You may also activate the credit monitoring and identity monitoring services we are making available to you. AUI will cover the cost of this service. Because the activation process does not allow us to activate on your behalf, you will need to activate yourself by following the instructions outlined in this letter

For More Information. We recognize that you may have questions not addressed in this letter. If you have additional questions, please contact 1-XXX-XXX-XXXX, Monday through Friday, 9:00 a.m. to 6:30 p.m., Eastern Time, excluding certain national U.S. holidays.

We take the privacy and security of the personal information in our care seriously, and sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Charles Plumhoff
Partner/CFO
AUI Partners, LLC

Steps You Can Take to Protect Personal Information

Activate Monitoring Services:

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 **June 28, 2021** to activate your identity monitoring services.*

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

Kroll | A Division of DUFF&PHELPS

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.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide 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, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

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

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, 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 Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your 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: 441 4th St. NW #1100 Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. AUI is located at 13600 Heritage Pkwy - Suite 150, Fort Worth, Texas 76177.

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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 73 Rhode Island residents impacted by this incident.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your 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 your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You 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 you to review your 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 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/.