LEWIS BRISBOIS BISGAARD & SMITH LLP

Robert L. Slaughter III
633 West 5th Street, Suite 4000
Los Angeles, California 90071
Robert.Slaughter@lewisbrisbois.com
Direct: 213.680.5028

January 18, 2021

VIA EMAIL
Attorney General Wayne Stenehjem
Office of the Attorney General
Consumer Protection and Antitrust
1050 East Interstate Avenue, Suite 200
Bismarck, ND 58503-5574
ndag@nd.gov

Re: Notification of Data Security Incident

Dear Attorney General Stenehjem:

Lewis Brisbois represents ALE Solutions, Inc. ("ALE") in connection with a data security incident as described in greater detail below. ALE is a company headquartered in St. Charles, Illinois, that works with insurance adjusters to coordinate temporary housing for families displaced from their homes. ALE 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 Data Incident.

In June 2020, ALE became aware of unusual activity within its network environment and discovered it had been the victim of data encryption by an unknown actor. Upon discovering this activity, ALE took immediate steps to secure its digital environment and promptly launched an investigation with the assistance of leading independent digital forensics and cybersecurity experts. ALE's investigation determined that, at some point between April and June of 2020, unauthorized parties may have accessed or acquired certain ALE data as a result of this incident. ALE promptly began a thorough review of the potentially affected data to identify any personal information that may have been contained therein, which concluded on December 16, 2020. ALE completed gathering up-to-date address information for the potentially affected individuals on January 8, 2021, at which time it learned that personal information belonging to eighteen North Dakota residents was contained within the potentially affected data. The potentially affected data sets for these individuals may have included the individuals' names and Social Security numbers.

2. Number of North Dakota Residents Potentially Affected.

ALE issued notification letters to the eighteen residents of North Dakota regarding this data security incident via first-class U.S. mail on January 11, 2020. A sample copy of the notification letter is attached hereto.

3. Steps Taken Relating to the Incident.

ALE has taken several steps to enhance the security of personal information in its possession in an effort to prevent similar incidents from occurring in the future. These measures include deploying an advanced threat detection tool with twenty-four hour active monitoring by a cybersecurity operations team, implementing hardened procedures for network administration, and implementing multifactor user authentication. ALE is also offering complimentary credit monitoring and identity theft protection services through TransUnion to all individuals potentially impacted by this incident, as an added layer of protection.

4. Contact Information.

ALE remains dedicated to protecting the personal information it maintains in its possession. If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at (213) 680-5028 or via email at Robert.Slaughter@lewisbrisbois.com.

Best regards,

Robert L. Slaughter III of
LEWIS BRISBOIS BISGAARD & SMITH LLP

RLS
Enclosure

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Subject: Notice of Data Security Incident

Dear <<Name 1>>,

I am writing to inform you of a data security incident that may have involved your personal information. At ALE Solutions, Inc. ("ALE"), we take the privacy and security of personal information very seriously. That is why I am notifying you of the incident, offering you credit monitoring and identity monitoring services, and informing you about steps you can take to help protect your personal information.

What Happened? ALE became aware of unusual activity within its network environment and discovered that it had been the victim of data encryption by an unknown actor. Upon discovering this activity, we took immediate steps to secure our environment and launched an investigation with the assistance of leading independent digital forensics and cybersecurity experts. Our investigation determined that unauthorized parties may have gained access to or downloaded certain ALE data as a result of this incident between April and June 2020. We promptly began a thorough review of the potentially affected data, which revealed that some of your personal information may have been contained therein. On December 16, 2020, we completed our review and gathering contact information needed to notify all potentially affected individuals.

ALE is committed to maintaining the security of all information within our possession. That is why we are contacting you, to offer you credit monitoring and identity protection services at no cost.

What Information Was Involved? The potentially affected information may include your name and Social Security number.

What Are We Doing? As soon as ALE discovered the incident, we took the measures described above. We have also improved our systems to reduce the likelihood of a similar incident occurring in the future. These improvements include deployment of an advanced threat detection tool with twenty-four hour active monitoring by a cybersecurity operations team, implementing hardened procedures for network administration, and implementing multifactor user authentication.

In addition, we are providing you with information about steps that you can take to help protect your personal information and, as an added precaution, we are offering you a one-year membership to TransUnion Interactive's *my*TrueIdentity credit monitoring and identity restoration service at no cost to you. This product provides you with premier credit monitoring and identity theft resolution, including up to $1 million of identity theft insurance coverage. To receive these services, you must be over the age of 18, 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. The deadline to enroll is **<<Enrollment Deadline>>**.

What Can You Do? You can follow the recommendations included with this letter to help protect your information. Specifically, we recommend that you review your credit report for unusual activity. If you see anything that you do not understand or that looks suspicious, you should contact the consumer reporting agencies for assistance using the contact information included with this letter. In addition, you can enroll in the free credit monitoring services that we are offering to you through TransUnion Interactive. Enrollment instructions are included with this letter.

We also recommend that you review the guidance included with this letter about how to protect your personal information.

For More Information: Further information about how to protect your personal information is included with this letter. If you have questions or need assistance, please contact 855-914-4694, Monday through Friday, 8:00 am – 8:00 pm CT. Our representatives are fully versed on this incident and can answer any questions you may have regarding the protection of your personal information.

We take your trust in us and this matter very seriously and we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Robert Zimmers, CEO
ALE Solutions, Inc.

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant, especially over the next 12 to 24 months, and review 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 should also 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 (the "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 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 can also contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-800-916-8800	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	www.annualcreditreport.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 90 days. 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: In some U.S. states, you have the right to put a security freeze on your credit file. 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. Contact information for the FTC is: Federal Trade Commission, 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov or www.ftc.gov/idtheft, 1-877-438-4338. Residents of New York, Maryland, North Carolina, and the District of Columbia can obtain more information from their Attorneys General using the contact information below.

New York Attorney General	Maryland Attorney General	North Carolina Attorney General	District of Columbia Attorney General
Bureau of Internet and Technology Resources	200 St. Paul Place	9001 Mail Service Center	400 6th Street NW
28 Liberty Street	Baltimore, MD 21202	Raleigh, NC 27699	Washington, D.C., 20001
New York, NY 10005	oag.state.md.us	ncdoj.gov	http://www.oag.dc.gov
ifraud@ag.ny.gov	1-888-743-0023	1-877-566-7226	202-727-3400
1-212-416-8433			

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

TransUnion

Activation Code: <<Activation Code>>

Complimentary One-year *my*TrueIdentity Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Insert static six-digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)