LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

January 29, 2020

VIA ELECTRONIC SUBMISSION

Wayne Stenehjem, Attorney General
Office of Attorney General
600 East Boulevard Avenue, Department 125
Bismark, ND 58505
Email: ndag@nd.gov

Re: Notification of Data Security Incident

Dear Attorney General Stenehjem:

.

We represent A&S Construction Co. ("A&S") in connection with a recent data security incident which is described in greater detail below. A&S, an affiliate of Ary Corporation, is based in Canon City, Colorado and supplies construction products and services to both private and public sector clients throughout Colorado and the surrounding states. A&S has taken steps to notify two (2) North Dakota residents potentially impacted in connection with this incident.

1. Nature of the security incident.

On September 16, 2019, A&S detected unusual activity pertaining to an A&S employee email account. Upon discovering this activity, A&S immediately took steps to secure the account and launched an investigation. In connection therewith, A&S engaged a leading, independent forensics firm to determine what happened and whether sensitive information had been accessed or acquired without authorization as a result. On December 30, 2019, the forensics firm reported that the A&S employee email account – which had been accessed by an unknown third-party without authorization – contained some personal information which may have been viewed or accessed by the unauthorized individual. The information potentially impacted as a result of this incident may have included notified individuals' names, dates of birth, Social Security numbers, and driver's license / government issued identification numbers.

2. Number of North Dakota residents affected.

A&S notified 2 North Dakota residents regarding this incident, whose information was contained within the accessed email account referenced above. Notification letters were mailed on January 29, 2020. A sample copy of the letter sent to potentially impacted individuals is enclosed.

3. Steps taken relating to the incident.

A&S 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 include, but are not limited to, mandating a password reset for the impacted email account and beginning to implement multi-factor authentication. A&S is also reviewing its procedures for handling and transmitting sensitive information, including personal information. Furthermore, A&S has offered potentially affected individuals complimentary credit monitoring and identity theft restoration services through Kroll, a global leader in risk mitigation and response.

4. Contact information.

A&S remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (720) 292-2052, or by e-mail at Alyssa.Watzman@lewisbrisbois.com.

.

Best regards,

Alyssa R. Watzman
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Consumer Notification Letter (Sample)

ARY
CORPORATION

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

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

Re: Notification of Data Security Incident

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

We are writing to inform you of a data security incident experienced by an affiliate of Ary Corporation, A&S Construction Co. ("A&S"), which may have affected your personal information. As explained below, we recently learned that an unauthorized individual gained access to an A&S employee email account containing your personal information. We are writing to notify you of this incident, to offer you complementary credit monitoring and identity theft restoration services, and to inform you about steps that can be taken to help protect your personal information.

What Happened? On September 16, 2019, we detected unusual activity pertaining to an A&S employee email account. Upon discovering this activity, we immediately took steps to secure the account and launched an investigation. In connection therewith, we engaged a leading, independent forensics firm to determine what happened and whether sensitive information had been accessed or acquired without authorization as a result. On December 30, 2019, the forensics firm reported that the A&S employee email account – which had been accessed by an unknown third-party without authorization – contained some of your personal information which may have been viewed or accessed by the unauthorized individual as a result of this incident.

Please note that this unauthorized access was limited to information transmitted via email and did not affect any other information systems. Moreover, we are not aware of the misuse of any of your personal information.

What Information Was Involved? The following information may have been contained within the accessed email account: your <<b2b_text_1(Impacted Data)>>.

What Are We Doing? As soon as we discovered this incident, we took the measures referenced above. We also implemented enhanced security measures applicable to our email system in order to better safeguard all information in our possession and to help prevent a similar incident from occurring in the future. Finally, we are offering you complementary identity monitoring services through Kroll, a global leader in risk mitigation and response. These services include Credit Monitoring, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

What Can You Do? We recommend that you activate your complementary Kroll services. Activation instructions and a description of the services being provided are included with this letter. We also recommend that you review the guidance included with this letter about how to help safeguard your personal information.

For More Information. If you have questions or need assistance, please contact Kroll at 1-877-514-0832, Monday through Friday from 7 a.m. to 4:30 p.m. Mountain Time, excluding major U.S. holidays. Kroll representatives are fully versed on this incident and can answer any questions you may have regarding the monitoring of your personal information and regarding the complementary services being offered to you.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Jodi Schreiber, COO
Ary Corporation

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 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 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 print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-877-322-8228	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	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 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. 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. There is no charge to place, lift or remove the security freeze. 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 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. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: 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 others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Kroll | A Division of DUFF & PHELPS

As referenced above, we have secured the services of Kroll to provide identity monitoring services at no cost to you. 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[1] include Credit Monitoring, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Services

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

*You have until **April 26, 2020** to activate your identity monitoring services.*

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

If you have questions, please call 1-877-514-0832, Monday through Friday from 7 a.m. to 4:30 p.m. Mountain Time.

Take Advantage of Your Services

You've 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 can help you determine if it's an indicator of identity theft.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for covered, out-of-pocket expenses totaling up to $1 million for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.