
1225 17th Street, Suite 2300
Denver, CO 80202-5596
TEL 303.292.2400
FAX 303.296.3956
www.ballardspahr.com

David M. Stauss
Tel: 303.299.7363
Fax: 303.296.3956
staussd@ballardspahr.com

March 1, 2018

Via E-mail and U.S. Mail

Attorney General Gordan MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification of Incident – ASI Constructors, Inc.

Dear Attorney General MacDonald:

We are providing notice on behalf of ASI Construction LLC (“ASI”) to the Office of the Attorney General, pursuant to N.H. REV. STAT. ANN. § 359-C:20(I)(b), of an incident involving nine (9) New Hampshire residents.

On January 31, 2018, ASI was the subject of a phishing attack which targeted employees’ 2017 W-2s. ASI’s information security team identified the perpetrating e-mail address on the same day of the incident, January 31, and reported the incident to the Federal Bureau of Investigation. No other company accounts or systems were impacted by the incident.

ASI has notified the Internal Revenue Service and state tax agencies of the incident in accordance with guidance provided by the IRS and has also implemented internal procedures to ensure that a similar incident does not occur. Additionally, ASI has secured an identity monitoring company to provide complimentary credit monitoring and identity protection services to individuals affected by the incident.

On Friday, March 2, ASI will notify the affected New Hampshire residents of the incident in accordance with N.H. REV. STAT. ANN. § 359-C:20. A sample copy of the notification letter is attached.

Please feel free to contact me if you have questions.

Respectfully yours,



David M. Stauss

DMS/dd

DMWEST #17470228 v1



ASI Construction LLC

1850 E. Platteville Blvd.
Pueblo West, CO 81007

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

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Re: Your Personal Information

Dear <<MemberFirstName>> <<MemberLastName>>,

We are writing to notify you of an incident that involved some of your personal information. We are notifying you as a precautionary measure, because we value and respect the privacy of your information.

WHAT HAPPENED? On January 31, 2018, an individual posing as John Bowen e-mailed an ASI Construction LLC employee requesting copies of 2017 W-2s for employees of ASI Constructors, Inc. Believing the sender to be John Bowen, the employee sent the requested 2017 W-2s of employees of ASI Constructors Inc. to that e-mail address. We believe your 2017 ASI Constructors, Inc. W-2 was among those sent.

WHAT INFORMATION WAS INVOLVED? A Form W-2 generally includes information about an employee's name, address, Social Security number, wages or other income and tax withholdings.

WHAT WE ARE DOING. We take this incident, and the security of your personal information, very seriously. Within hours of discovering this incident, our IT department identified the perpetrating e-mail address and reported the incident to the Federal Bureau of Investigation. We also contacted the e-mail service provider and confirmed that it froze the e-mail account. No other company accounts or systems were impacted by the incident.

Since the incident, we notified the Internal Revenue Service and state tax agencies according to the guidance provided by the IRS. We also implemented additional procedures to ensure that a similar incident does not occur.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. 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, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit krollbreach.idMonitoringService.com to activate and take advantage of your identity monitoring services. You have until **May 31, 2017** to activate your identity monitoring services.

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-844-263-8605. Additional information describing your services is included with this letter.

WHAT YOU CAN DO. We are notifying you about this incident so you may take appropriate steps to protect your information. We recommend that you review the enclosed "Additional Resources" which includes recommendations by the Internal Revenue Service and Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. We also recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your account statements, and monitoring free credit reports for any unauthorized activity. If you find any unauthorized or suspicious activity, you should contact your credit card company or financial institution immediately.

To ensure all appropriate steps are taken to protect your information, we also recommend that you utilize the complementary, two (2)-year subscription to the Kroll identity monitoring services noted above by following the enclosed instructions for enrollment.

FOR MORE INFORMATION. The security of our employees' personal information has been and remains our highest priority. If you have any questions, please feel free to contact 1-866-775-4209, Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time. Please have your membership number ready.

We understand the importance of protecting the privacy and security of your personal information, and we take our obligations seriously. We apologize for any inconvenience this issue may cause you.

Sincerely,

James F. Cunningham
General Counsel



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ 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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses 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 Internet Explorer, Chrome, Firefox, and Safari. 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.

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, P.O. Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, P.O. Box 2002, Allen, TX 75013, www.experian.com, 1-877-322-8228

TransUnion, P.O. Box 1000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and regularly monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at 1-877-322-8228.

You can also request your free annual credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:

You may obtain one or more (depending on your state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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 see to obtain credit.

Security Freeze. You can 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 may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. To place a freeze by telephone, contact:

Equifax: 1-800-349-9960

Experian: 1-888-397-3742

TransUnion: 1-888-909-8872

You must have the following information when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (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; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The credit reporting agencies may charge a fee to place a freeze, temporarily lift it or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigation or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.)

For Massachusetts residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is \$5.00.

For Rhode Island residents: If you are the victim of identity theft, the placement, temporary lifting, and removal of a credit freeze is free. If you are not a victim of identity theft the placement and temporary lifting of a credit freeze is \$10.00, removing the credit freeze is free.

Fair Credit Reporting Act. You have certain rights under the Fair Credit Reporting Act, including (1) to be told if information in your file has been used against you, (2) to know what is in your file, (3) to ask for your credit score, and (4) to dispute incomplete or inaccurate information and have it corrected or deleted.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338)

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-8777-566-7226.

For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 1-401-274-4400.

Reporting of identity theft and obtaining a police report.

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

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

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

For Rhode Island residents: You have the right to file or obtain a policy report if you are a victim of identity theft.

Internal Revenue Service. The Internal Revenue Service has published the following guidance for individuals involved in a W-2 data loss:

1. Review the Taxpayer Guide to Identity Theft, which is available online at: www.irs.gov/newsroom/taxpayer-guide-to-identity-theft
2. Review IRS Publication 5027 ("Identity Theft Information for Taxpayers"), which is available online at www.irs.gov/pub/irs-pdf/p5027.pdf The IRS recommends that individuals review the section entitled "Steps for Identity Theft Victims," which includes information about how to contact credit bureaus to place a fraud alert or credit freeze on your account; for filing a complaint with the FTC, and directs individuals to review the information provided by the FTC at www.identitytheft.gov for additional steps to recover from identity theft.
3. Review IRS Publication 4524 ("Security Awareness for Taxpayers"), which is available online at <https://www.irs.gov/pub/irs-pdf/p4524.pdf>.

Please do not hesitate to contact us if you would prefer to receive hard copies of these documents.