



David B. Sherman
550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
David.Sherman@lewisbrisbois.com
Direct: 215.977.4070

April 15, 2019

VIA E-MAIL

Attorney General Gordon J. MacDonald
Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification of Data Security Incident

Dear Attorney General MacDonald:

We represent Assemblers, Inc. ("Assemblers") with respect to a recent data security incident described in greater detail below. Assemblers takes the protection of sensitive information very seriously and is taking steps to prevent similar incidents from occurring in the future.

1. Nature of the security incident.

On February 18, 2019, Assemblers learned that wage and tax information for certain current and former Assemblers employees was inadvertently disclosed via e-mail to an unauthorized individual in error on February 12, 2019. Upon discovering this information, Assemblers launched an internal investigation and contacted the e-mail recipient. The results of that investigation indicate that the names, addresses, Social Security numbers, and tax and wage information for certain current and former Assemblers employees was involved.

2. Number of New Hampshire resident(s) affected.

Assemblers notified one (1) resident of New Hampshire regarding this data security incident via first class U.S. mail on April 15, 2019. A sample copy of the notification letter sent to the potentially impacted individual is included with this letter.

3. Steps taken relating to the incident.

Assemblers has taken steps in response to this incident to prevent similar incidents from occurring in the future. Those steps include reprimanding and retraining the employee who inadvertently disclosed sensitive information and supplementing its security protocols. In addition, while Assemblers is currently not aware of any misuse of information, out of an abundance of caution, Assemblers is providing twelve (12) months of credit and identity monitoring services to each letter recipient at no cost through Kroll, a global leader in risk mitigation and response. Those services include credit monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, fraud consultation, and identity theft restoration.

4. Contact information.

Assemblers 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 (215) 977-4070 or by e-mail at David.Sherman@lewisbrisbois.com.

Respectfully,



David B. Sherman of
LEWIS BRISBOIS BISGAARD & SMITH LLP

DBS:arb

Encl.: Consumer Notification Letter



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

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Subject: Notification of Data Security Incident

Dear <<FirstName>> <<LastName>>,

I am writing to inform you of a data security incident that involved your personal information. Assemblers, Inc. (“Assemblers”) takes the privacy and security of your information very seriously. That is why we are contacting you, offering you complimentary credit and identity monitoring services, and informing you about steps that can be taken to help protect your personal information.

What Happened? On February 18, 2019, we learned that Form W-2 Wage and Tax Statement information for certain current and former Assemblers employees was inadvertently disclosed via e-mail to an unauthorized individual in error on February 12, 2019. Upon discovering this information, we immediately launched an internal investigation and contacted the e-mail recipient. In addition, we reprimanded and retrained the employee who accidentally disclosed the information, and supplemented our security protocols to help minimize the likelihood of a similar incident from occurring again.

Assemblers is not currently aware of any misuse of your personal information. Nonetheless, out of an abundance of caution, we are notifying you of this incident and are providing you with access to twelve months of credit and identity monitoring services at no cost to you, described in further detail below.

What Information Was Involved? The information involved Form W-2 Wage and Tax Statement information which included your name, address, Social Security number, and tax and wage information.

What Are We Doing? As soon as we discovered the incident, we immediately took the steps described above. We are also 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 complimentary credit and identity monitoring services through Kroll for twelve (12) months. 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 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 **July 11, 2019** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-866-359-5414. Additional information describing your services is included with this letter.

What You Can Do: You can follow the recommendations on the following page to help protect your personal information. You can also contact Kroll with any questions by calling our dedicated call center at 1-866-359-5414.

For More Information: We remain committed to protecting your information. If you have any questions regarding this incident or the services being provided to you, please contact our dedicated call center at 1-866-359-5414, from 8:00 a.m. to 5:30 p.m., Central Time, Monday through Friday. Please have your Membership Number, <<Member ID>>, ready.

Thank you for your patience through this incident. We take your trust in us and this matter very seriously. Please accept our apologies for any worry or inconvenience this may cause you.

Sincerely,

A handwritten signature in black ink that reads "Tina M. Belau". The signature is written in a cursive, flowing style.

Tina M. Belau
Senior Manager, HR & Compliance | Assemblers, 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 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	1-877-322-8228	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: 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 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 and North Carolina can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	Maryland Attorney General	North Carolina Attorney General
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699
consumer.ftc.gov , and	Marylandattorneygeneral.gov	ncdoj.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226
1-877-438-4338		

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>.

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.