



Maxwell J. Petersen
550 West Adams Street, Suite 300
Chicago, Illinois 60661
Maxwell.Petersen@lewisbrisbois.com
Direct: 312.463.3386

March 13, 2017

File No. 39395.13

VIA E-MAIL

Iowa Attorney General Tom Miller
Consumer Protection Division
Security Breach Notifications
Office of The Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
Email: consumer@iowa.gov

Re: Data Security Incident

Dear Attorney General Miller:

We represent Faller, Kincheloe & Co., PLC ("FKC"), an accounting firm located in Des Moines, Iowa. This letter is being sent pursuant to Iowa Code §§715C.1 and 715C.2 because FKC determined on February 4, 2017 that personal information of 3,229 Iowa residents may have been involved in a data security incident. The information which may have been involved includes tax return information, including names, addresses, dates of birth, social security numbers, and bank account numbers.

FKC believes this data security incident was connected to a malicious hacking that occurred on February 4, 2017. On that day, FKC lost access to its information system. FKC immediately contacted their information technology provider, who disabled and isolated affected devices and disconnected the system from the internet. Over the next 10 days, FKC's information technology provider rebuilt their network and created new internal accounts with new passwords and other security measures. On February 16, 2017, FKC was notified by an Internal Revenue Service Criminal Investigation (IRS/CI) Agent that a small number of clients' tax returns had been filed using FKC's Electronic Filing Identification Number, without FKC's authorization. FKC has since been working with the IRS/CI to prevent fraudulent returns from being accepted or refunds issued, and to hold the perpetrators accountable.

ARIZONA • CALIFORNIA • COLORADO • CONNECTICUT • FLORIDA • GEORGIA • ILLINOIS • INDIANA • KANSAS • KENTUCKY

LOUISIANA • MARYLAND • MASSACHUSETTS • MISSOURI • NEVADA • NEW JERSEY • NEW MEXICO • NEW YORK

4844-9933-8565.1

March 13, 2017
Page 2

FKC has also notified the affected customers via the attached letter. As referenced in the letter, FKC is offering 12 months of credit and identity monitoring services through Kroll, a risk mitigation company. Please contact me if you have any questions.

Sincerely,

/Maxwell J. Petersen/
Maxwell J. Petersen for
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl. Consumer Notification Letter



<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Date>> (Format: Month Day, Year)
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Subject: Data Security Incident

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

I am writing to inform you of a data security incident that may have affected your personal information. We take the privacy and security of your information very seriously. This is why I am contacting you, offering you credit and identity monitoring services, and informing you about steps that can be taken to protect your personal information.

What Happened? On February 4, 2017, we experienced a data security incident that prevented access to our information system. We immediately contacted our information technology provider who disabled and isolated affected devices and disconnected the system from the Internet. Over the next ten days, our information technology provider rebuilt our network and created new internal accounts with new passwords and other security measures. On February 16, 2017, we were notified by an Internal Revenue Service Criminal Investigation (IRS/CI) Agent that a small number of tax returns had been filed with our Electronic Filing Identification Number without our authorization. It appears that at least a small number of client files were accessed without authorization. While there is no evidence that anyone has used your information, we wanted to inform you of the incident and encourage you to utilize the services referenced below to protect your personal information.

What Information Was Involved? The following information may have been accessed: tax return information which included names, addresses, dates of birth, and Social Security numbers.

What Are We Doing? As soon as we detected a data security incident, we took the steps referenced above. We will provide the IRS/CI whatever cooperation is necessary to prevent fraudulent returns from being accepted or refunds issued, and to hold the perpetrators accountable. We are also providing you information about steps you can take to protect your personal information, and are offering you credit and identity monitoring services for 12 months at no cost to you. We have also enhanced the security of our systems, making it more difficult for similar incidents to occur in the future.

What You Can Do: You can follow the recommendations on the following page to protect your personal information. You can also enroll in the services we are offering through Kroll, a global leader in risk mitigation and response, to monitor your identity for 12 months at no cost to you. 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. You must enroll in the services by June 9, 2017, and they can be used for 12 months thereafter. They will include Credit Monitoring, Web Watcher, Fraud Consultation, and Identity Theft Restoration. Visit <http://kroll.idmonitoringservice.com> to take advantage of your services. Your membership number is <<Member ID>>. To receive credit services by mail instead of online, please call 1-855-656-6589.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, call 1-855-656-6589, 8:00 a.m. to 5:00 p.m. (Central Time), Monday through Friday. Kroll's licensed investigators are standing by to assist you. Please have your membership number ready. You may also contact Alan Kincheloe at Faller, Kincheloe & Co if you prefer.

If you haven't already done so, we also encourage you to complete IRS Form 14039, Identity Theft Affidavit which you can obtain at <http://www.irs.gov/pub/irs-pdf/f14039.pdf>, and then mail or fax it to the IRS according to instructions on the form. Please contact us should you need assistance filing Form 14039. If you have other identity theft/tax related issues, contact the IRS Identity Protection Specialized Unit at 1-800-908-4490.

We are grateful for your business and your trust. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Alan Kincheloe", written in a cursive style.

Alan Kincheloe, CPA

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:

| 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 | 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 US 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. If you request a security freeze from a consumer reporting agency there may be a fee up to \$10 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, Federal Trade Commission 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 Federal Trade Commission 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 Washington, DC 20580 consumer.ftc.gov , and www.ftc.gov/idtheft 1-877-438-4338 | 200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023 | 9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226 | 150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 401-274-4400 |



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Credit Monitoring through TransUnion

You'll 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.

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 will do most of the work for you. Your investigator can dig deep to uncover all aspects 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.

AG CONSUMER [AG]

From: Petersen, Maxwell <Maxwell.Petersen@lewisbrisbois.com>
Sent: Monday, March 13, 2017 5:57 PM
To: AG CONSUMER [AG]
Subject: Data Security Incident
Attachments: Letter to Iowa Attorney General.docx; Faller Kincheloe Co Ad Not Affected r4.pdf.pdf

Dear Mr. Miller:

Please see attached letter and enclosure.

Best Regards,

Max Petersen

Maxwell J. Petersen
Partner
Maxwell.Petersen@lewisbrisbois.com
Lewis Brisbois Bisgaard & Smith LLP
550 West Adams Street, Suite 300
Chicago, IL 60661
T:312.463.3386 F: 312.345.1778

www.LewisBrisbois.com

This e-mail may contain or attach privileged, confidential or protected information intended only for the use of the intended recipient. If you are not the intended recipient, any review or use of it is strictly prohibited. If you have received this e-mail in error, you are required to notify the sender, then delete this email and any attachment from your computer and any of your electronic devices where the message is stored.