

BakerHostetler

RECEIVED

OCT 12 2020

CO! Baker & Hostetler LLP

2929 Arch Street  
Cira Centre, 12th Floor  
Philadelphia, PA 19104-2891

T 215.568.3100  
F 215.568.3439  
www.bakerlaw.com

Eric A. Packel  
direct dial: 215.564.3031  
epackel@bakerlaw.com

October 9, 2020

**VIA OVERNIGHT MAIL**

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

*Re: Incident Notification*

Dear Sir or Madam:

We are writing on behalf of our client, RSC Insurance Brokerage, Inc. and its division, Weaver Brothers, (collectively "RSC"), to notify you of a security incident.

RSC completed its investigation of an incident that involved unauthorized access to an employee's email account. RSC began its investigation after phishing emails were sent from the employee's email account. Upon learning of this, RSC immediately reset the password to the employee's email account and launched an investigation, with the assistance of a cyber security firm.

Through its investigation, which was completed on August 12, 2020, RSC determined that there was unauthorized access to the employee's email account on May 6, 2020. RSC's investigation indicated that the likely purpose of the unauthorized access to the employee's email account was to simply send additional phishing emails and not to view or use any information in the account. However, due to the lack of definitive evidence one way or the other, RSC could not rule out the possibility that some emails may have been viewed or accessed during the incident.

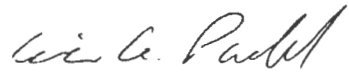
Accordingly, as part of its investigation, RSC conducted a comprehensive review of the emails and attachments in the employee's email account to identify individuals whose information may have been subject to unauthorized access as a result of this incident. The investigation determined that some emails in the account contained personal information, including names and driver's license numbers.

Beginning on October 9, 2020, RSC will mail a notification letter via United States Postal Service First-Class mail to one resident in accordance with N.H. Rev. Stat. Ann. § 359-C:20. A copy of the notification letter is enclosed. RSC is offering the New Hampshire resident a complimentary one-year membership in credit monitoring and identity theft protection services from Kroll. To help prevent something like this from happening again, RSC is reevaluating its existing security protocols and is reinforcing education with its employees on how to identify and avoid phishing emails.

Attorney General Gordon MacDonald  
October 9, 2020  
Page 2

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in cursive script, appearing to read "Eric A. Packel".

Eric A. Packel

Enclosure



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

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country >>

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>:

RSC Insurance Brokerage, Inc. and our division, Weaver Brothers, (collectively “RSC”) are committed to protecting the confidentiality of the information we maintain. We are writing to inform you of an incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

RSC completed its investigation of an incident that involved unauthorized access to an employee’s email account. RSC began its investigation after phishing emails were sent from the employee’s email account. Upon learning of this, we immediately reset the password to the employee’s email account and launched an investigation, with the assistance of a leading cyber security firm.

Through our investigation, which was completed on August 12, 2020, we determined that there was unauthorized access to the employee’s email account on May 6, 2020. Our investigation indicated that the likely purpose of the unauthorized access to the employee’s email account was to simply send additional phishing emails and not to view or use any information in the account. However, due to the lack of definitive evidence one way or the other, we could not rule out the possibility that some emails may have been viewed or accessed during the incident.

Accordingly, as part of our investigation, we conducted a comprehensive review of the emails and attachments in the employee’s email account to identify individuals whose information may have been subject to unauthorized access as a result of this incident.

Our investigation determined that some of your information was contained in the email account, and may have included your name in combination with your <<b2b\_text\_1 (Impacted Data)>>.

We recommend you remain vigilant to the possibility of fraud by reviewing your financial account and payment card statements for any suspicious activity. You should immediately report any suspicious activity to your financial institution.

As a precaution, we have secured the services of Kroll to provide identity monitoring at no cost to you for a period of one year. 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, Fraud Consultation, and Identity Theft Restoration. **For more information about Kroll’s identity monitoring, including instructions on how to activate your complimentary one-year membership, please visit the below website:**

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

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

Membership Number: <<Member ID>>

We deeply regret any concern or inconvenience this incident may cause you. To help prevent something like this from happening again, we are reevaluating our existing security protocols and are reinforcing education with our employees on how to identify and avoid phishing emails. If you have any questions about this incident, please call 1-888-498-0911, Monday through Friday, between 9:00 a.m. and 6:30 p.m., Eastern Time.

Sincerely,

*Richard T. West, Jr.*

Richard T. West, Jr.  
Managing Director



## ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any 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 companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

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 in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**Fraud Alerts:** There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report. For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

**Credit or Security Freezes:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit. There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)

You'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request. If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

### **Additional information for residents of the following states:**

**Maryland:** RSC's mailing address is 160 Federal St, Boston, MA 02110. You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, [www.oag.state.md.us](http://www.oag.state.md.us)

**New York:** You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>* and *New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>*

**North Carolina:** You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, [www.ncdoj.gov](http://www.ncdoj.gov)*

**A Summary of Your Rights Under the Fair Credit Reporting Act:** The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to [www.consumerfinance.gov/learnmore](http://www.consumerfinance.gov/learnmore) or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit “prescreened” offers of credit and insurance you get based on information in your credit report.
- You have a right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.



## **TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES**

You have been provided with access to the following services from Kroll:

### **Triple Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

### **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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

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.