

RECEIVED

APR 04 2019

BakerHostetler

CONSUMER PROTECTION

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

April 3, 2019

VIA OVERNIGHT MAIL

Attorney General Gordon MacDonald
New Hampshire 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, Re-Solutions, ("RSC") to notify you of a security incident. RSC assists healthcare providers and health insurance plans with purchasing reinsurance policies.

On April 2, 2019, RSC mailed notification letters via United States Postal Service First-Class mail to eight (8) New Hampshire residents¹ in accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (45 C.F.R. § 164.404) and N.H. Rev. Stat. § 359-C:20. A copy of the notification letter is enclosed.

On January 22, 2019, RSC provided written notification to its healthcare provider and health insurance plan clients that it had completed its investigation and analysis of an incident involving the theft of an RSC employee's password-protected laptop. The laptop was stolen on August 23, 2018. In the notification to its healthcare provider and health insurance plan clients, RSC offered to provide notice to their patients, insureds, and applicable regulatory agencies on their behalf. Thereafter, the various RSC clients responded affirmatively to the notification offer over several weeks. Then, through April 2, 2019, RSC worked with its clients to complete the notice process, including identifying the addresses for individuals to be notified.

Note that RSC has no evidence that any files or documents on the stolen laptop were ever viewed or accessed by any unauthorized individual. The information involved varied per individual, but included names along with dates of birth, Social Security numbers, health insurance claims information, diagnoses, and treatment information. RSC offered individuals whose Social Security numbers were potentially involved complimentary one-year memberships in credit monitoring and identity theft protection services

¹ Notice is also being provided to 3 additional New Hampshire residents whose names, dates of birth, medical information and health insurance plan numbers were contained in files on the stolen laptop, in accordance with 45 C.F.R. § 164.404. This information does not trigger notice obligations under N.H. Rev. Stat. § 359-C:20.

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

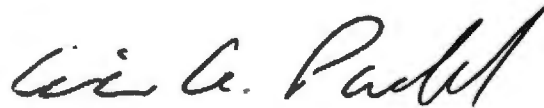
New Hampshire Office of the Attorney General
April 3, 2019
Page 2

from Experian®. RSC has also provided a telephone number for individuals to call with any questions they may have.

To help prevent a similar incident from occurring in the future, RSC is enhancing security measures on its devices that store personal information.

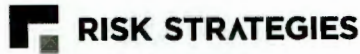
Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

A handwritten signature in black ink, appearing to read "Eric A. Packel". The signature is written in a cursive style with a large, sweeping initial "E".

Eric A. Packel

Enclosure



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

Dear <<Name 1>>:

Re-Solutions, a division of RSC Insurance Brokerage, Inc. ("RSC"), provides services to your healthcare provider, and maintains information related to those services. We are writing to inform you about an incident involving some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

On January 22, 2019, RSC provided written notification to your healthcare provider that it had completed its investigation and analysis of an incident involving the theft of an RSC employee's password-protected laptop. The laptop was stolen on August 23, 2018. Upon learning of the theft, RSC notified law enforcement, changed the employee's account credentials, and launched an investigation with the assistance of a leading cyber security firm. After completing a comprehensive review of the files that may have been contained on the stolen laptop, RSC determined that the laptop may have contained your name, <<variable data>>

Although, to date, we have no evidence that any of your information was actually viewed, accessed, or has been misused, out of an abundance of caution, we wanted to let you know this happened and assure you we take it very seriously. We recommend that you regularly review the explanation of benefits received from your health insurer. If you see services that you did not receive, please contact the insurer immediately. As a precaution, we have secured the services of Experian® to offer you a complimentary one-year membership of Experian's IdentityWorksSM. This product helps detect possible misuse of your information and provides you with identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks is completely free and enrolling in this program will not hurt your credit score. **For more information on IdentityWorks, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take to protect yourself, please see the pages that follow this letter.** Identity restoration assistance is immediately available to you.

We regret any inconvenience or concern this may cause you. To help prevent a similar incident from occurring in the future, we are enhancing security measures on our devices that store personal information.

If you have any questions, please call 877-213-1934, or 877-213-1937 (TTY), Monday through Friday, 9:00 a.m. to 9:00 p.m., Eastern Time.

Sincerely,

Anthony Plampton

Anthony Plampton
Managing Director
RSC Insurance Brokerage, Inc.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

1. ENROLL by: <<Enrollment Deadline>> (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: www.experianidworks.com/3bcredit
3. PROVIDE the **Activation Code**: <<Activation Code>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877-890-9332**. Be prepared to provide engagement number <<Engagement Number>> as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at www.experianidworks.com/3bcredit or call 877-890-9332 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at **877-890-9332**.

* ~~Offline members~~ will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE

Regardless of whether you choose to take advantage of the complimentary credit monitoring, we recommend that you remain 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 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, 1-800-685-1111

Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, 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, www.ftc.gov/idtheft, 1-877-IDTHEFT (438-4338)

If you are a resident of Maryland, Massachusetts, North Carolina, or Rhode Island, you may contact and obtain information from your state attorney general at:

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202 www.oag.state.md.us, 1-888-743-0023 (toll free when calling within Maryland) 1-410-576-6300 (for calls originating outside Maryland)

Massachusetts Office of the Attorney General, One Ashburton Place, Boston, MA 02108, www.mass.gov/ago/contact-us.html, 1-617-727-8400

North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400 or toll free at 1-877-566-7226

Rhode Island Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400

Note that pursuant to **Massachusetts and Rhode Island law**, you have the right to file and obtain a copy of any police report.

If you are a resident of West Virginia, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

Fraud Alerts: There are two types of 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 at least 90 days. 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. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain 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:

Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com
Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five years, provide the addresses where you have lived over the prior five years
5. Proof of current address such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (<https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>), and that article refers individuals seeking more information to visit www.ftc.gov/credit.

The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Experian, TransUnion and Equifax – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you're on welfare; or if your report is inaccurate because of fraud, including identity theft.
- 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 may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.