

BakerHostetler

RECEIVED

JUL 24 2019

CONSUMER PROTECTION
Baker & Hostetler LLP

Key Tower
127 Public Square, Suite 2000
Cleveland, OH 44114-1214

T 216.621.0200
F 216.696.0740
www.bakerlaw.com

David E. Kitchen
direct dial: 216.861.7060
dkitchen@bakerlaw.com

July 23, 2019

Via overnight mail

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

Re: Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of our client, Sterling & Sterling, LLC d/b/a SterlingRisk ("SterlingRisk"), and one of its clients, to notify your office of a security incident involving 12 New Hampshire residents.¹

SterlingRisk provides insurance-based services to a variety of clients. To accomplish this function, SterlingRisk receives from, or on behalf of, its clients, necessary data about policy participants, including certain types of personal information.

On May 24, 2019, SterlingRisk began contacting clients that had provided SterlingRisk with personal information that was involved in an email phishing incident. SterlingRisk offered to provide notification to each clients' individuals whose information was contained in the email account, as well as complimentary credit monitoring services for eligible individuals, call center services, and required regulator notifications. SterlingRisk is now providing notice to individuals whose information was provided to SterlingRisk by a client who accepted SterlingRisk's offer. Twelve of these individuals have been identified to be New Hampshire residents. These individuals' information includes their names and Social Security numbers.

SterlingRisk contacted its clients shortly after completing its forensic investigation into an email phishing incident that resulted in an unauthorized person gaining access to an email account belonging to a SterlingRisk employee on April 3, 2019. After learning of the incident, SterlingRisk immediately took steps necessary to secure the employee's email account and promptly engaged a leading cyber security firm to assist with an investigation. The investigation was not able to determine which personal information, if any, was viewed or acquired by the unauthorized person. Because SterlingRisk could not rule out that possibility, it reviewed the full contents of the employee's email account.

¹ SterlingRisk is notifying the New Hampshire residents on behalf of LAZ Karp Associates, LLC.

July 23, 2019

Page 2

On July 23, 2019, SterlingRisk will begin mailing notification letters via United States Postal Service First-Class mail to the 12 New Hampshire residents, in accordance with N.H. Rev. Stat. Ann. § 359-C:20.² A copy of the notification letter is enclosed. If any additional client accepts SterlingRisk's offer with respect to a New Hampshire resident, SterlingRisk will provide notice to such individuals in the same manner.

SterlingRisk has established a dedicated call center that individuals may call with related questions, and it is offering individuals whose Social Security numbers were contained in the email account with one year of complimentary credit monitoring and identity theft protection services through Experian's® IdentityWorksSM. The notification letter provides a toll-free number to call with questions about the credit monitoring services.

To help prevent a similar incident from occurring in the future, SterlingRisk is implementing additional security enhancements and providing additional education and training to our employees.

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 "David E. Kitchen", with a long horizontal line extending to the right.

David Kitchen

Enclosure

² This report is not a waiver of SterlingRisk's objection that New Hampshire lacks personal jurisdiction regarding the company related to this matter.



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>>:

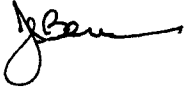
SterlingRisk provides or has provided insurance-based services to a variety of clients and other parties, including <<Client>>. SterlingRisk recognizes the importance of protecting the privacy of personal information provided to us by such clients and third parties. We are writing to inform you that we recently identified and addressed a security incident that may have involved some of your information that <<Client>> provided to us. This notice describes the incident, outlines the measures we have taken in response, and advises you on steps that you can take to help protect your information.

On April 17, 2019, we completed our forensic investigation into an email phishing incident and determined that an unauthorized person gained access to an email account belonging to a SterlingRisk employee on April 3, 2019. After learning of the incident, SterlingRisk immediately took steps necessary to secure the employee's email account and promptly engaged a leading cyber security firm to assist with an investigation. Our investigation was not able to determine whether your personal information was actually viewed or acquired. Because we cannot completely rule out that possibility, we reviewed the full contents of the employee's email account for personal information. Our review found that an email or an attachment in the employee's email account contained your <<Data Elements>>.

We encourage you to remain vigilant for incidents of fraud or identity theft by reviewing your account statements for any unauthorized activity. You also should review the additional information on the following pages on ways to protect yourself. As a precaution, we are offering you a complimentary one-year membership with Experian's® IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorksSM Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. **For more information on IdentityWorksSM, 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 additional information provided in this letter.**

We apologize for any inconvenience or concern this incident may cause. To help prevent something like this from happening in the future, we are implementing additional security enhancements and providing additional education and training to our employees. If you have any questions about this matter, please call 1-855-424-1297, Monday through Friday between 9:00 am and 9:00 pm Eastern Time.

Sincerely,

A handwritten signature in black ink, appearing to read 'J. Beres', with a long horizontal flourish extending to the right.

John S. Beres
Executive Vice President

Activate IdentityWorks Credit 3B Now in Three Easy Steps

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: <<Enrollment 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 by <<Enrollment Deadline>>. 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.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for two years from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* 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.

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

Regardless of whether you choose to take advantage of this complimentary credit monitoring service, we remind you to 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:

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

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

If you are a resident of Maryland or North Carolina 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) or 410-576-6300 (for calls originating outside Maryland)

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

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:

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

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.