



MULLEN
COUGHLIN_{LLC}

STATE OF NH
DEPT OF JUSTICE

2017 MAY -9 PM 1:51

Ryan C. Loughlin
Office: 267-930-4786
Fax: 267-930-4771
Email: rloughlin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

May 5, 2017

VIA U.S. MAIL

Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General Foster:

Our office represents RM Acquisition, LLC d/b/a Rand McNally (“Rand McNally”), 9855 Woods Drive, Skokie, Illinois 60077. In follow-up to the notice provided to your office on behalf of Rand McNally on March 16, 2017, we are writing to provide you with supplemental notice of the incident described in Rand McNally’s previous correspondence. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Rand McNally does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Background

Rand McNally became aware of suspicious activity on a server for its e-commerce store, www.RandMcNally.com and commenced an investigation. A third-party forensic investigation firm was retained to assist with this investigation. On April 11, 2017, Rand McNally confirmed there was unauthorized remote access to the e-commerce store server beginning on April 12, 2016, which resulted in the installation of malware on the server. It was further determined that between April 12, 2016 and March 2, 2017, the malware collected or may have collected data relating to customers who made purchases through the e-commerce store using a credit or debit card.

From the company’s investigation, it appears that the only customer information collected by the malware was first and last name, address, phone number, and credit or debit card information, including card number, expiration date, and Card Verification Value (“CVV”) number. No PINs, Social Security numbers, bank account information (other than credit card numbers) or health information was collected by the malware, as Rand McNally does not accept this type of

information from its customers during the e-commerce checkout process. Rand McNally's investigation found evidence that information relating to several hundred e-commerce customers had been collected by the malware. However, there was evidence found indicating that the responsible actor had repeatedly accessed collected customer information and deleted evidence of such collected data. Therefore, the investigation cannot rule out unauthorized access to and acquisition of information relating to customers who made purchases between April 12, 2016 and March 2, 2017.

Notice to New Hampshire Residents

On May 5, 2017, Rand McNally mailed written notice to approximately 131 New Hampshire residents whose personal information may have been collected by the malware between April 12, 2016 and March 2, 2017. Such notice was in substantially the same form as the letter template attached here as *Exhibit A*.

Other Steps Taken and to Be Taken

Rand McNally is offering all potentially affected individuals access to 1 year of free identity monitoring and identity restoration services through Experian, as well as a hotline to contact with questions or concerns regarding this incident. Additionally, Rand McNally is providing potentially impacted individuals with helpful information on how to protect against identity theft and fraud, including how to place a fraud alert and security freeze on one's credit file, the contact information for the national consumer reporting agencies, how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, state attorney general, and law enforcement to report attempted or actual identity theft and fraud.

Rand McNally is also providing written notice of this incident to other state regulators and the major consumer reporting agencies, as necessary.

Contact Information

Should you have any questions regarding this notification of other aspects of this event, please contact us at 267-930-4786.

Very truly yours,



Ryan Loughlin of
MULLEN COUGHLIN LLC

RCL:ab
Enclosure

Exhibit A



RAND McNALLY

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

<<Mail ID>>
<<Name>>
<<Address1>>
<<Address2>>
<<City>><<State>> <Zip>>

<Date>>

Re: Notice of Data Breach

Dear Rand McNally Customer:

We know this is not news you want to receive. At Rand McNally, we'd much rather be sending you information about the best small towns to visit or tips to help you plan your next vacation.

However, we are writing to inform you of the possible unauthorized acquisition of your personal credit card information, what that means to you, how we are actively addressing the situation, and what you might do to protect yourself. If you have experienced any fraudulent charges on your card, the bank that issued the card may have already replaced your card and/or caught the charges on its own.

What Happened?

On February 28, 2017, we became aware of suspicious activity on the server for our e-commerce store. When you purchased anything via this website you entered information, including your credit card and other personal information. Through this breach, an unauthorized party may have been able to gain access to your credit card information by installing malware that obtained that information. Though we believe this party may have first gained access to credit card information around April 2016, we only recently discovered on or around April 11, 2017 that your information may have been collected as a result of the incident.

What Type of Information Was Involved?

The information that may have been collected included demographic information and personal credit card information such as billing and shipping address, phone number, the cardholder name, card number, card type, expiration date and CVV for transactions made between April 12, 2016 and March 2, 2017.

What We Are Doing

As soon as we discovered the unauthorized access, we began investigating the server and removed the malware to prevent any further potential access. We worked with leading cyber investigators to determine what happened and what information may be affected. The incident and pertinent details are being reported to the appropriate agencies, and we are fully cooperating with them. We have also been notifying those who may be affected as they are identified and providing them with information on the incident and what they can do to protect against possible fraud.

What You Can Do

Because Rand McNally takes the protection of your personal security very seriously, we are offering you access to 1 year of complimentary identity monitoring and identity restoration services through Experian at no cost to you. Information on these services and how you can enroll to receive them immediately are included within the enclosed *Steps You Can Take to Further Protect Yourself*.

For More Information

If you have questions or concerns that are not addressed in this letter, you may call the dedicated assistance line we've established regarding this incident. You may call the assistance line at 888-746-7079, Monday through Friday, 9:00 a.m. to 9:00 p.m. EDT (excluding U.S. holidays).

We apologize for any inconvenience this may have caused. Be assured that we have been working, and will continue working, diligently to avoid and mitigate any harm to you

Sincerely,



Stephen A. Fletcher
CEO

STEPS YOU CAN TAKE TO FURTHER PROTECT YOURSELF

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. If, after discussing your situation with an agent, it is determined that identity restoration support is needed, an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (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 offer is available to you for one-year 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.

While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorksSM as a complimentary one-year membership. This product provides you with internet surveillance, and identity theft insurance at no cost to you upon enrollment. To start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by:** <<Enrollment Deadline>> (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/identityone
- Provide your **activation code:** <<Enrollment Code>>

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident, 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 Membership:

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

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related 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.

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.

* 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

In addition to the above offer of services, we are providing this explanation of steps you can take to protect your information. As a precautionary measure, we recommend that you remain vigilant for incidents of fraud and identity theft by reviewing your account statements and credit reports closely. If you believe that your credit or debit card has been used, you should immediately contact your credit card company. The phone number to call is usually on the back of the credit or debit card. You may obtain a free copy of your credit report from each of the three major credit reporting agencies listed below once every 12 months by visiting <http://www.annualcreditreport.com> or calling toll-free 1-877-322-8228. You can also report any fraudulent activity or any suspected identity theft to proper law enforcement authorities, your state attorney general and/or the Federal Trade Commission. To file a complaint about identity theft with the FTC or to learn more, go to www.identitytheft.gov, call 1-877-ID-THEFT (1-877-438-4338).

Fraud Alert

We suggest you 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. If you would like to place a fraud alert on your credit report, contact any of the three credit reporting agencies using the contact information below. The Federal Trade Commission has a good website with an overview and guidance on this issue at <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>. You can also contact them at: Federal Trade Commission or write to: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Or, call 1-877-ID-THEFT.

Security Freeze Information

In some US states, you have the right to place 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. You can obtain further information regarding security freezes from the FTC and from any of the three credit reporting agencies listed below.

Equifax
(800) 685-1111
(NY residents please call 1-800-349-9960)
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian
(888) 397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion
(888) 909-8872
www.transunion.com
P.O. Box 2000
Chester, PA 19016

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that they have been a victim. Instances of known or suspected identity theft should be reported to local law enforcement or your state Attorney General. This notice was not delayed by law enforcement.

For Maryland Residents:

You may contact the Maryland Attorney General's Office, General Consumer Protection Division, at 1-888-743-0023, www.oag.state.md.us, or 200 St. Paul Place, Baltimore, MD 21202.

For North Carolina Residents:

You may contact North Carolina Office of the Attorney General at <http://www.ncdoj.gov/Crime.aspx>. Call 1-919-716-6400 or write to: Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001.

For Rhode Island Residents:

You may contact the Rhode Island Attorney General by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of approximately (57) Rhode Island residents may be impacted by this incident.