



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED

AUG 31 2018

CONSUMER PROTECTION

Jeffrey J. Boogay
Office: 267-930-4784
Fax: 267-930-4771
Email: jboogay@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

August 27, 2018

INTENDED FOR ADDRESSEE(S) ONLY
VIA U.S. MAIL

Attorney General Gordon J. MacDonald
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 MacDonald:

Our firm represents Salter Labs, 272 East Deerpath Rd, Suite 302, Lake Forest, IL 60045 ("Salter"), and write to notify your office of an incident that may affect the security of personal information relating to certain approximately three (3) New Hampshire residents. By providing this notice, Salter does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about April 17, 2018, Salter discovered that it had been the target of an email phishing campaign that resulted in the compromise of an employee's email account credentials. Salter immediately took steps to secure the employee's email account and launched an in-depth investigation to determine the full nature and scope of the event. This investigation included working with third party computer forensic investigators.

Through the investigation, Salter determined that an unauthorized actor gained access to the Salter employee's email account beginning on or around April 9, 2018. The investigation also determined that the emails affected by this incident contained personal information. With the assistance of third party forensic investigators, Salter worked diligently to determine what personal information was present in the email account and to whom those records relate. While the investigation to date has no evidence that any information potentially affected by this event has been misused, it was unable to rule out that information in the account was accessed by the unauthorized actor.

The investigation has confirmed that the following types of information related to New Hampshire residents may be impacted by this event: name, security code/pin, credit/debit card number, and credit/debit card expiration date.

Notice to New Hampshire Residents

On August 27, 2018, Salter will begin providing written notice of this incident to all affected individuals, which includes approximately three (3) New Hampshire residents. Written notice will be provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the email phishing campaign, Salter immediately launched an investigation to determine what happened and ensure that the unauthorized access to the email account was terminated. Salter also changed the employee's passwords. Salter then worked diligently, with the assistance of third party forensic investigators, to confirm the full nature and scope of the event, determine what personal information was present in the email account, and identify to whom those records relate.

Salter is also providing notice to all potentially affected individuals. This notice will include an offer of access to one (1) free year of credit and identity monitoring services, including identity restoration services, through Kroll Inc. Additionally, Salter is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on 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, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Salter is also providing written notice of this incident to the consumer reporting agencies and other state regulators as necessary.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4784.

Very truly yours,



Jeffrey J. Boogay of
MULLEN COUGHLIN LLC

EXHIBIT A



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

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Re: Notice of Data Breach

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

We write to inform you of a recent event that may affect the security of your personal information. While we are unaware of any actual or attempted misuse of your personal information, out of an abundance of caution, we are providing you with information about the incident, steps we are taking in response, and steps you can take to protect against potential misuse of your information, should you feel it is appropriate.

What Happened? On or about April 17, 2018, we discovered that Salter Labs had been the target of an email phishing campaign that resulted in the compromise of an employee’s email account credentials. We immediately took steps to secure the employee’s email account and launched an in-depth investigation to determine the full nature and scope of the event. This investigation included working with third party computer forensic investigators.

Through the investigation, we determined that an unauthorized actor gained access to the Salter Labs employee’s email account beginning on or around April 9, 2018. The investigation also determined that the emails affected by this incident contained personal information. With the assistance of third party forensic investigators, we worked diligently to determine what personal information was present in the email account and to whom those records relate. While we currently have no evidence that any information potentially affected by this event has been misused, we were unable to rule out that information in the account was accessed by the unauthorized actor.

What Information Was Involved? Based on the investigation, we have confirmed that your <<ClientDef1(data elements affected)>>, and name were present in the affected email account at the time of this event.

What We Are Doing. We take the security and privacy of information in our care very seriously. Since discovering this event, we have been working diligently, with third-party forensic investigators, to determine what happened and what information was accessible to the unauthorized actor. This has involved a diligent forensic investigation, as well as a comprehensive programmatic and manual review of the data in the affected email account to identify potentially sensitive records. We are providing notice of this event to you, and to certain regulators and consumer reporting agencies as required.

We are also providing you with notice of this incident and will be notifying state regulators as required by law. As an added precaution, we are offering you access to 12 months of credit monitoring, fraud consultation, and identity theft restoration services through Kroll at no cost to you. The cost of this service will be paid by Salter Labs. We encourage you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service.

What You Can Do. You can enroll and receive the free credit monitoring and identity restoration services we are offering. You can also review the enclosed “Privacy Safeguards Information” for additional information on how to better protect your personal information.

For More Information. We apologize for any inconvenience or concern this incident causes you. The security of your information is a priority to us. Should you have any questions about the content of this letter or ways you can better protect yourself from the possibility of identity theft, please call 1-???-???-??? between 9:00 am and 6:00 pm ET, Monday through Friday, excluding major holidays.

Sincerely,

A handwritten signature in black ink that reads "Angela J. Perkins". The signature is written in a cursive, flowing style.

Angela Perkins
Chief Financial Officer
Salter Labs

PRIVACY SAFEGUARDS INFORMATION

Enroll in Credit Monitoring:

Visit <<IDMonitoringURL>> to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter. We encourage you to review the description and to consider enrolling in this product. You must complete the enrollment process by no later than <<Date>>.

Monitor Your Accounts:

Credit Reports and Account Statements. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus listed below directly to request a free copy of your credit report.

Fraud Alerts. At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
800-680-7289
www.transunion.com

Security Freeze. You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. Fees vary based on where you live, but commonly range from \$3 to \$15. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
freeze.transunion.com

Additional Information. You can further educate yourself regarding identity theft, security freezes, fraud alerts, and the steps you can take to protect yourself against identity theft and fraud by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should be promptly reported to law enforcement, the Federal Trade Commission, and your state Attorney General. This notice has not been delayed as the result of a law enforcement investigation.

For Maryland residents, the Maryland Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. The Salter Labs is located at 272 East Deerpath Rd, Suite 302, Lake Forest, IL 60045.

For North Carolina residents, the North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General can be contacted 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 <<NUMBER>> Rhode Island residents are potentially impacted by this incident. You have the right to file and obtain 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 you have been a victim.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Single Bureau Credit Monitoring

You will 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.

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 can dig deep to uncover the scope 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.