



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED
APR 15 2019
CONSUMER PROTECTION

Brian F. Fox
Office: (267) 930-4777
Fax: (267) 930-4771
Email: bfox@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

April 11, 2019

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:

We represent The Shubert Organization, Inc. ("Shubert"), located at 234 West 44th Street, New York, NY 10036. We are writing to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, ("Shubert") 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 February 11, 2019, Shubert became aware of unusual activity related to an employee's email account. Shubert immediately launched an investigation, with the aid of forensic experts, to determine the nature and scope of the activity. With the computer forensic firm, Shubert learned of unauthorized access to some employees' email accounts. The unauthorized access occurred between February 8, 2019 to February 11, 2019. Shubert undertook a lengthy and labor-intensive process to identify the personal information contained in the affected email accounts. While the investigation was unable to confirm the scope of the information that was accessed within the affected email accounts, Shubert is notifying one (1) New Hampshire resident in an abundance of caution because Shubert was able to confirm on March 14, 2019, that this individual's information was present in the affected email accounts.

The information that could have been subject to unauthorized access includes name and Social Security number.

Notice to New Hampshire Residents

On or about April 12, 2019, Shubert provided written notice of this incident to all affected individuals, which includes one (1) New Hampshire resident. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

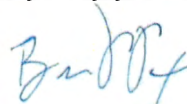
Upon discovering the event, Shubert moved quickly to investigate and respond to the incident, assess the security of Shubert systems, identify the individuals potentially affected by this incident, and notify potentially affected individuals. Shubert is providing access to credit monitoring services for two (2) years, through TransUnion Interactive, to potentially affected individuals, at no cost to these individuals. Shubert also continues to assess and update its employee training and security measures in response to the incident.

Additionally, Shubert is providing potentially affected individuals with guidance on how to better protect against identity theft and fraud, including advising the individuals to report any suspected incidents of identity theft or fraud to their institution, provider, credit card company and/or bank. Shubert is also providing the potentially affected individuals with 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, the state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4777.

Very truly yours,



Brian F. Fox of
MULLEN COUGHLIN LLC

BFF/crm
Enclosure

EXHIBIT A



The Shubert
Organization
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>>

Re: Notice of Data Breach

Dear <<Name 1>>:

The Shubert Organization, Inc. ("Shubert") recently discovered an incident that may affect the security of your personal information. We write to provide you with information about the incident, steps we are taking in response, and steps you can take to better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so.

What Happened? On or about February 11, 2019, Shubert became aware of unusual activity related to an employee's email account. Shubert immediately launched an investigation, with the aid of forensic experts, to determine the nature and scope of the activity. With the computer forensic firm, Shubert learned of unauthorized access to some employees' email accounts. The unauthorized access occurred between February 8, 2019 to February 11, 2019. Shubert undertook a lengthy and labor-intensive process to identify the personal information contained in the affected email accounts. While the investigation was unable to confirm the scope of the information that was accessed within the affected email accounts, Shubert is notifying you in an abundance of caution because we have confirmed that your information was present in the affected email accounts.

What Information Was Involved? Shubert was unable to confirm whether your information was actually accessed by the unauthorized individual. However, on March 14, 2019 our investigation confirmed that the information present in the affected email accounts includes your <<Variable Data>>.

What We Are Doing. We take the security of personal information in our care very seriously. We have security measures in place to protect the data on our systems and we continue to assess and update our security measures and training to our employees to safeguard the privacy and security of information in our care. This incident has been reported to certain state regulators, and Attorneys General.

We are providing you with access to twenty-four (24) months of complimentary credit monitoring services through TransUnion Interactive.

What You Can Do. We encourage you to enroll in the twenty-four (24) months of credit monitoring services through TransUnion Interactive. Please review the enclosed "Steps You Can Take to Protect Against Identity Theft and Fraud," which contains instructions on how to enroll and receive the complimentary credit monitoring services.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If so, you may contact our call center at 855-795-3708, which is available Monday through Friday from 9:00 A.M. to 9:00 P.M. Eastern Time.

We regret any concern or inconvenience this has caused you.

Sincerely,

THE SHUBERT ORGANIZATION, INC.

Steps You Can Take to Protect Against Identity Theft and Fraud

Shubert is providing you with access to twenty-four (24) months of an online credit monitoring service (*myTrueIdentity*) provided by TransUnion Interactive, a subsidiary of TransUnion,[®] one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code <<**12-letter Activation Code**>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode <<**Telephone Pass Code**>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<**Enrollment Deadline**>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. 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 directly to request a free copy of your credit report.

You have the 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. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

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

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

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 (5) 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 either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, 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 also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

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 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.

For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are two (2) Rhode Island residents impacted by this incident.