



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED

MAY 14 2019

CONSUMER PROTECTION

Christopher J. DiLenno
Office: (267) 930-4775
Fax: (267) 930-4771
Email: cdiienzo@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

May 10, 2019

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General Gordon J. MacDonald:

We represent The Southeastern Council on Alcoholism and Drug Dependence, Inc (“SCADD”) located at 37 Camp Mooween Road, Lebanon, CT 06249 and write to notify your office of an incident that may affect the security of some personal information relating to thirteen (13) New Hampshire residents. 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, SCADD 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 February 18, 2019, SCADD discovered certain disruptions in its network. Upon further review, it was determined that its systems were infected with ransomware. SCADD immediately began an investigation to determine the nature and scope of the event. This investigation included working with third-party forensic experts. Once SCADD systems were secure, its efforts focused on determining what information was impacted, to whom the information related, and valid address information for those individuals to notify them of the event. The investigation did not determine that personal information was, in fact, accessed or acquired, but the possibility of such exists and could not be ruled out.

Notice to New Hampshire Residents

On or about April 19, 2019 SCADD began providing written notice of this incident to affected individuals, which includes thirteen (13) New Hampshire residents. 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, SCADD moved quickly to investigate and respond to the incident, assess the security of SCADD systems, and notify potentially affected individuals. SCADD is also working to implement additional safeguards and training to its employees. SCADD is providing access to credit monitoring services for twelve (12) months, through Kroll to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, SCADD is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. SCADD is providing 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, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. SCADD is also providing notice of this event to the Department of Health and Human Services, as well as other state regulators as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4775.

Very truly yours,



Christopher J. DiIenno of
MULLEN COUGHLIN LLC

CJD/acl

EXHIBIT A



Southeastern Council.

Alcoholism and Drug Dependence, Inc.

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

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

The Southeastern Council on Alcoholism and Drug Dependence, Inc. ("SCADD") writes to make you aware of a recent event that may affect the privacy of some of your personal information. While there is currently no evidence that your information has been misused, we are making you aware of the event, the steps we are taking in response, and steps you may take to better protect against possible misuse of your personal information, should you feel it appropriate to do so.

What Happened? On February 18, 2019, SCADD discovered certain disruptions with its network. Upon further review, it was determined that our systems were infected with ransomware. SCADD immediately began an investigation to determine the nature and scope of the event. This investigation included working with third-party forensic experts. Once SCADD systems were secure, our efforts focused on determining what information was potentially impacted, to whom the information related, and valid address information for those individuals to notify them of the event.

What Information Was Involved? Through the ongoing investigation, SCADD determined that the information present on its systems impacted by this event may include your name, address, Social Security number, as well as medical history and treatment information. To date, SCADD has not received any reports of actual or attempted misuse of your personal information as a result of this event.

What We Are Doing. SCADD takes the confidentiality, privacy, and security of patient information in our care seriously. Upon learning of this event, we commenced an investigation to confirm the nature and scope of the incident and immediately took steps to ensure that our systems were secure. As part of the investigation, SCADD began efforts to identify the personal information stored on systems affected by this event and we are notifying the individuals who are potentially affected. While SCADD has security measures in place to protect patient information in our care, we are taking steps to implement additional safeguards, as well as review policies and procedures relating to data privacy and security. SCADD is also notifying the required regulators of the event including the Department of Health and Human Services.

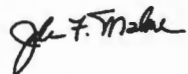
As an added precaution, SCADD is providing you with access to twelve (12) months of identity monitoring services from Kroll at no cost to you. A description of services and instructions on how to enroll can be found within the enclosed Steps You Can Take to Protect Against Identity Theft and Fraud. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf.

What You Can Do. You can review the enclosed Steps You Can Take to Protect Against Identity Theft and Fraud. You can also enroll to receive the free identity monitoring services through Kroll.

For More Information. We understand you may have questions about this event that are not addressed in this letter. If you have questions or concerns, please call our dedicated hotline at 1-???-???-???, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time.

Please know SCADD takes the privacy and security of patient information in our care very seriously and we sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "J. F. Malone". The signature is fluid and cursive, with the first name "Jack" and last name "Malone" clearly legible.

Jack Malone
Chief Executive Officer
The Southeastern Council on Alcoholism and Drug Dependence

STEPS YOU CAN TAKE TO PROTECT AGAINST IDENTITY THEFT AND FRAUD

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

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>>

To receive credit services by mail instead of online, please call 1-???-???-?????. Additional information describing your services is included with this letter.

Monitor Your Accounts

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 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 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

TransUnion

P.O. Box 2000

Equifax

P.O. Box 105069

Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud

Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal

Additional Information

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); 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 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. The Southeastern Council on Alcoholism and Drug Dependence is located at 37 Camp Mooween Road Lebanon, Connecticut 06249.

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 Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are XXX Rhode Island residents impacted by this incident.



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.