



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED
DEC 11 2017
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

December 6, 2017

INTENDED FOR ADDRESSEE(S) ONLY

VIA US 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 Mr. MacDonald:

We represent Bennington-Rutland Supervisory Union, 6378 Vermont Route 7A, Sunderland, VT 05250, and are writing to notify your office of an incident that may affect the security of personal information relating to eighteen (18) New Hampshire residents. The investigation into this incident is ongoing, and this notice will be supplemented with any substantive information learned after submission of this notice. By providing this notice, Bennington-Rutland Supervisory Union 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 July 6, 2017, Bennington-Rutland Supervisory Union discovered its computer system had been infected with a virus that prohibited access to its files. The integrity of the computer system was immediately restored and an investigation was launched with the assistance of a forensic expert, to determine the capabilities of the virus and how it was introduced to the system. As part of the extensive investigation, on September 27, 2017, it was determined that this virus was introduced by an unknown third party that had access to a server on Bennington-Rutland Supervisory Union's computer system.

Notice to New Hampshire Residents

While the investigation is ongoing, and there is no evidence the unknown third party viewed or took information stored on the server, it has been confirmed that this server housed files and a

software application containing information which may have included the names, dates of birth, addresses, drivers' license numbers and Social Security numbers relating to eighteen (18) residents of New Hampshire. On or about December 6, 2017, Bennington-Rutland Supervisory Union is providing written notice of this incident to potentially impacted individuals in substantially the same form as the letter attached hereto as *Exhibit A*.

Other Steps Taken and To Be Taken

Bennington-Rutland Supervisory Union is providing potentially impacted individuals access to 2 free years of credit monitoring and restoration services through TransUnion, and has established a dedicated hotline for individuals to contact with questions or concerns regarding this incident. Additionally, Bennington-Rutland Supervisory Union 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. Bennington-Rutland Supervisory Union is also providing written notice of this incident to consumer reporting agencies and 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,

A handwritten signature in black ink, appearing to read 'C. Dilenno', with a stylized flourish at the end.

Christopher J. Dilenno of
MULLEN COUGHLIN LLC

Exhibit A

BENNINGTON-RUTLAND SUPERVISORY UNION

Return Mail Processing Center

PO 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 <<Name1>>:

I am writing to inform you of a recent event that may affect the security of your personal information. As an employee or vendor of Bennington-Rutland Supervisory Union or one of the school districts it oversees, you provided Bennington-Rutland Supervisory Union with certain 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. We are also providing you with information regarding the steps we are taking in response, and steps you can take to protect against fraud should you feel it is appropriate.

What Happened? On July 6, 2017, we discovered our computer system had been infected with a virus that prohibited our access to our files. We immediately restored our computer system and launched an investigation, with the assistance of a forensic expert, to determine the capabilities of the virus and how it was introduced to our system. As part of our extensive investigation, on September 27, 2017, we determined that this virus was introduced by an unknown third party that had access to a server on our computer system, and that information relating to you was stored on this system. While there is a potential that this third party gained access to your personal information, we are currently unaware of any attempted or actual access or misuse of your information has occurred.

<<Data Element Paragraph>>

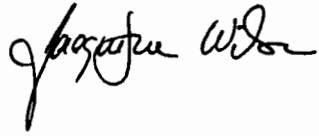
What the Supervisory Union Is Doing? We take this matter, and the security and privacy of information on our information system, very seriously. Since the incident occurred, we have further enhanced the security of the computer system and implemented additional monitoring tools to detect suspicious activity. We are also providing notice of this incident, as well as complimentary access to credit monitoring and identity restoration services and information on what you can do to better protect against the possibility of identity theft and fraud, to you.

What Can You Do? While we have no evidence your information was subject to unauthorized access, or that your information has been or will be misused, you can take steps to better protect against the possibility of identity theft and fraud by enrolling to receive the complimentary credit monitoring and identity restoration services we are offering to you. You can also review the additional information on protecting against misuse of your information. This additional information, as well as instructions on how to enroll and receive the complimentary monitoring and restoration services, are included in the attached Privacy Safeguards.

For More Information. We understand you may have questions relating to this event and this letter. We have established a privacy line staffed with individuals familiar with this incident and how to better protect against the possibility of identity theft and fraud, and you can direct all questions and concerns to this line by calling 844-853-3576, between 9:00 a.m. and 9:00 p.m. EST, Monday through Friday, excluding major holidays.

We apologize for any inconvenience this incident may cause you, and remain committed to the privacy and security of our information.

Sincerely,

A handwritten signature in black ink, appearing to read "Jacquelyne Wilson". The signature is fluid and cursive, with the first name being more prominent.

Jacquelyne Wilson
Superintendent
Bennington-Rutland Supervisory Union

PRIVACY SAFEGUARDS

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for two years provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

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 following 12-letter Activation Code <<Insert Unique 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 following 6-digit telephone pass code <<Insert static 6-digit 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 <<Insert Date>>. 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.

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, change 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 to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

In addition to enrolling to receive the free monitoring and restoration services we are offering to you, we encourage you to remain vigilant against incidents of identity theft and financial loss by reviewing your account statements and monitoring your credit reports for suspicious activity. Under U.S. law, everyone is entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit <http://www.annualcreditreport.com/> or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report:

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 19022
800-680-7289
www.transunion.com

At no charge, you can also have these credit bureaus place a "fraud alert" on your credit file. A "fraud alert" will tell creditors to take additional steps to verify your identity prior to granting credit in your name; however, because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the credit bureaus verify your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your files. You may use the contact information listed above to contact the major credit bureaus and place a "fraud alert" on your credit report.

You can also place a "security freeze" on your credit file that prohibits a credit bureau from releasing any information from your credit report without your written authorization but may delay, interfere with, or prevent the timely approval of any requests for new credit. If you have been a victim of identity theft, and provide the credit bureau with

a valid police report, the credit bureau cannot charge 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. If you incur a cost to place a security freeze, please let us know. You must contact each of the credit bureaus separately to place a security freeze on your credit file:

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

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

TransUnion
PO Box 2000
Chester, PA 19022-2000
1-888-909-8872
www.transunion.com/securityfreeze

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. **For Maryland residents**, the 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. **For North Carolina residents**, the 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 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 Rhode Island residents may be impacted by this incident.

Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. This notice was not delayed as the result of a law enforcement investigation.