MULLEN COUGHLIN
ATTORNEYS AT LAW

RECEIVED
JAN 31 2022
CONSUMER PROTECTION
NH DEPT OF JUSTICE
JAN 31 2022 PM 12:43

Samuel Sica, III
Office: (267) 930-4802
Fax: (267) 930-4771
Email: ssica@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

January 25, 2022

VIA U.S. MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent Midland University ("Midland") located at 900 North Clarkson Street, Fremont, NE 68025, and are writing to notify your office of an event that may affect the security of certain personal information relating to approximately four (4) New Hampshire residents. This notice may be supplemented if any new significant facts are learned subsequent to its submission. By providing this notice, Midland 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 January 18, 2021, Midland discovered that its network had been impacted by a sophisticated malware attack that encrypted certain computer files. Midland immediately launched an investigation, with the assistance of third-party computer forensic specialists, to determine the nature and scope of the event and notified federal law enforcement. Midland also worked quickly to: (1) secure its systems; (2) restore access to the information so Midland could continue to operate without disruption, and (3) investigate what happened and whether the event resulted in any unauthorized access to, or theft of, information by the unknown actor. Through the investigation, Midland determined that the unknown actor gained access to certain files on January 18, 2021 and downloaded a subset of those files.

Midland then worked with third-party data review specialists to perform a comprehensive programmatic and manual review of the affected files to determine what information was impacted and to whom the information related. Upon completion of the third-party review, Midland then

conducted a time-intensive manual review of its records to determine the identities and contact information for potentially affected individuals. On or around December 22, 2021, Midland concluded its review.

The information that could have been subject to unauthorized access for New Hampshire residents includes name, address, Social Security number, and driver's license or state identification number.

Notice to New Hampshire Residents

On or about January 25, 2022, Midland provided written notice of this event to affected individuals, which includes approximately four (4) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached hereto as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Midland moved quickly to investigate and respond, assess the security of Midland systems, and notify potentially affected individuals. Midland implemented additional technical and administrative safeguards and training to its employees. Midland has also engaged third-party cybersecurity specialists to provide ongoing information technology and security services. To date, Midland has not received any indication of identity theft or fraud as a result of this event. In an abundance of caution, Midland is providing access to credit monitoring and identity restoration services for one (1) year, through Equifax, to individuals whose personal information was potentially affected by this event, at no cost to these individuals. Midland also established a dedicated assistance line to respond to questions or concerns from potentially affected individuals.

Additionally, Midland 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. Midland is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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. Midland also notified other appropriate government regulators.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4802.

Very truly yours,

Samuel Sica, III of
MULLEN COUGHLIN LLC

SZS/dtg
Enclosure

EXHIBIT A

MIDLAND UNIVERSITY

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>>

<<Mail Date>>

<<Variable Header>>
Dear <<Name 1>>:

Midland University ("Midland") is writing to inform you of an event that may impact the security of some of your information. While we have received no indications of actual misuse of your information as a result of this event, this notice provides information about the event, our response, and resources available to you to help protect your information from possible misuse, should you feel it appropriate to do so.

What Happened? On January 18, 2021, Midland identified that its network had been impacted by a malware attack that encrypted certain files. We immediately launched an investigation to determine the nature and scope of the event. We quickly worked to: (1) secure our systems; (2) restore access to the information so we could continue to operate without disruption, and (3) investigate what happened and whether the event resulted in any unauthorized access to, or theft of, information by the unknown actor. Through our investigation, we determined that the unknown actor gained access to certain files on January 18, 2021 and downloaded a subset of those files.

We then worked with third-party specialists to perform a comprehensive review of the affected files to determine what information was impacted and to whom the information related. Upon completion of the review, we then conducted a time-intensive manual review of our records to determine the identities and contact information for potentially affected individuals. On or around December 22, 2021, we confirmed address information for affected individuals to provide notifications.

What Information Was Involved. Our investigation determined that the impacted information may have included your name and <<Breached elements>>.

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this incident very seriously. We reviewed our security policies and procedures to reduce the risk of similar future events. **Although we do not have any indication of identity theft or fraud as a result of this event**, we are offering complimentary credit monitoring and identity restoration services through Equifax for <<CM Length>> months as an added precaution. We also reported this event to federal law enforcement and notified appropriate state regulators.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and free credit reports for suspicious activity and to detect errors. Additional information and resources are included in the enclosed *Steps You Can Take to Protect Personal Information*. You may also enroll in the complementary credit monitoring services available to you. Enrollment instructions are enclosed with this letter.

For More Information. If you have additional questions, please call our dedicated assistance line at 855-604-1768, Monday through Friday (excluding U.S. holidays), during the hours of 8:00 a.m. to 8:00 p.m., Central Time. You may also write to Midland at 900 North Clarkson, Fremont, NE 68025.

We sincerely regret any inconvenience or concern this event may cause.

Sincerely,

Jodi Benjamin

Jodi Benjamin
Chief Operating Officer
Midland University

Steps You Can Take to Protect Personal Information

Enroll in Credit Monitoring

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of <<ACTIVATION CODE>>, with an Enrollment Deadline of <<Enrollment Deadline>>, then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

   You're done!
   The confirmation page shows your completed enrollment.
   Click "View My Product" to access the product features.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and 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 bureaus 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 New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There is 1 Rhode Island resident impacted by this incident.