

RECEIVED

JUN 08 2021

CONSUMER PROTECTION



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Sian M. Schafle
Office: (267) 930-4799
Fax: (267) 930-4771
Email: sschafle@mullen.law

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

June 4, 2021

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 DeSales University (“DeSales”) located at 2755 Station Ave., Center Valley, PA 18034, and are writing to notify your office of an incident that may affect the security of some personal information relating to twenty-two (22) New Hampshire residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, DeSales 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 September 23, 2020, DeSales discovered suspicious activity in its network. DeSales immediately launched an investigation and worked closely with third-party forensic specialists to determine the nature and scope of this activity. The investigation determined that files stored on certain DeSales systems were accessed without authorization from September 3, 2020 to September 24, 2020. On October 25, 2020, the investigation determined that a DeSales employee email account was also potentially accessed without authorization sometime between July 14, 2020 and September 29, 2020.

DeSales worked diligently with third-party forensic specialists to conduct a comprehensive review of the involved systems including a review for sensitive information. This review concluded on or around March 23, 2021. The personal information as defined by N.H. Rev. Stat. Ann. § 359-C:19(IV)(a) that was identified in the involved systems includes name and Social Security number.

Notice to New Hampshire Residents

On June 4, 2021, DeSales mailed written notice of this incident to approximately twenty-two (22) 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

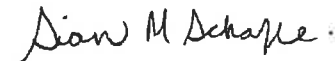
Upon discovering the event, DeSales moved quickly to investigate and respond to the incident, assess the security of DeSales systems, and notify potentially affected individuals. DeSales is also working to implement additional safeguards and training to its employees. DeSales is providing access to credit monitoring services for one (1) year through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, DeSales is providing impacted individuals with guidance on how to better protect against identity theft and fraud. DeSales 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4799.

Very truly yours,



Sian M. Schafle of
MULLEN COUGHLIN LLC

SMS:mep

EXHIBIT A



DESALES 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>>

<<Date>>

<<Variable Header>>

Dear <<Name 1>>:

DeSales University (“DeSales”) is writing to inform you of an incident that may affect the security of some of your personal information. This notice provides information about the incident previously communicated to the campus community on September 29, 2020, DeSales’ response, and resources available to you to help protect your information, should you feel it necessary to do so. While DeSales has found no evidence of unauthorized activity to date, we want to ensure we are taking every precaution to protect your personal information.

What Happened? On September 23, 2020, DeSales discovered suspicious activity in its network. DeSales immediately launched an investigation and worked closely with third-party forensic specialists to determine the nature and scope of this activity. The investigation determined that files stored on certain DeSales systems were accessed without authorization from September 3, 2020 to September 24, 2020. On October 25, 2020, the investigation determined that a DeSales employee email account was also potentially accessed without authorization sometime between July 14, 2020 and September 29, 2020.

We worked diligently with third-party forensic specialists to conduct a comprehensive review of the involved systems including a review for sensitive information. The review of this matter concluded on or around March 23, 2021.

What Information is Involved? The information found in the involved files and/or email account includes your name and <<Data Elements>>. DeSales has found no evidence of actual or attempted misuse of your personal information to date.

What Are We Doing To Protect You? We take this incident and the security of your personal information seriously. Upon learning of this incident, we moved quickly to investigate and respond to this incident, assess the security of our systems, and notify potentially affected individuals. We notified law enforcement and relevant regulators. As part of our ongoing commitment to IT security, we are reviewing and enhancing existing policies and procedures with the support of leading third-party security experts to reduce the likelihood of a similar future event.

As an added precaution, we are offering complimentary credit monitoring and identity protection services for <<CM Length>> months through TransUnion. These services include fraud consultation and identity theft restoration services. If you wish to activate the credit monitoring and identity protection services, you may follow the instructions included in the *Steps You Can Take to Help Protect Your Information*.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and credit reports for suspicious activity. You may also review the information contained in the attached *Steps You Can Take to Help Protect Your Information*. There you will also find more information on the credit monitoring and identity protection services we are making available to you. While DeSales will cover the cost of these services, you will need to complete the activation process.

As communicated in the September 29, 2020 memorandum to the campus community, all DeSales users were required to update their password credentials. We recommend that you change your password every 180 days in accordance with our policy. If you reuse your DeSales University username and password for any other online accounts, it is recommended that you change the password and any security question or answer for those online accounts, as well. Further, as a general precaution, you should never use the same password for more than one online account. When creating passwords, they should be complex and not contain personal information.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our call center at 855-654-0922 between 9:00 a.m. and 9:00 p.m. Eastern Time, Monday through Friday. You may also write to DeSales at 2755 Station Ave., Center Valley, PA 18034.

Sincerely,

A handwritten signature in black ink, appearing to read "Robert Snyder", written in a cursive style.

Robert Snyder
Vice President for Finance and Administration
DeSales University

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

Complimentary *myTrueIdentity* Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for <<CM Length>> months provided by TransUnion Interactive, a subsidiary of TransUnion,⁶ 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 <<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 six-digit telephone passcode <<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 <<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 COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain <<CM Length>> months 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.)

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 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 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 fraud alert or 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. DeSales is located at 2755 Station Ave., Center Valley, PA 18034.

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 are nine (9) Rhode Island residents impacted by this incident.

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 violators. 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/>.