

MATTHEW C. SPAULDING  
419.321.1455  
mspaulding@shumaker.com

August 4, 2020

**VIA EMAIL ONLY**

Attorney General Wayne Stenehjem  
Office of the North Dakota Attorney General  
Consumer Protection and Antitrust Division  
1050 E. Interstate Avenue, Suite 200  
Bismarck, ND 58503-5574  
ndag@nd.gov

Re: Data Breach Notification  
Our File No. 222421

Dear Attorney General Stenehjem

This firm represents St. John's Jesuit High School & Academy ("St. John's"), which is located in Toledo, Ohio, regarding a data security incident involving a third party service provider as more fully described below.

On July 16, 2020, St. John's received notification from a third party service provider that the service provider suffered a ransomware attack at some point beginning on February 7, 2020 and continuing intermittently until May 20, 2020. In connection with this attack, our service provider has advised that a copy of backup data, which contained personal information concerning our alumni and donors may have been compromised in the attack. The types of information potentially compromised include first and last name, mailing address, email address, business organization name, business mailing address, title, industry, profession, income, date of birth, check numbers for any applicable donations, donation history, names of family members who also attended St. John's, tuition amounts charged, any financial aid awarded, and record of payments (i.e. date and amounts).

St. John's has identified two North Dakota residents whose personal information may have been impacted by this data security incident. On August 4, 2020, St. John's notified both of these North Dakota residents of the data security incident by first class U.S. mail. Please find the enclosed copy of the notification letter, which was sent to these residents.

The Honorable Attorney General Way Stenehjem

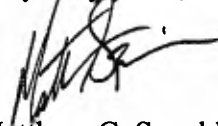
August 4, 2020

Page 2

Our service provider has advised that they have already implemented several changes to protect data from any subsequent incidents, including by identifying and fixing the vulnerability that was exploited by the cybercriminal in this instance and confirming that the repair withstands all known tactics. St. John's is re-evaluating the types of data it collects and maintains regarding alumni and donors moving forward and its data security requirements for vendors.

If you have any questions or require additional information about the aforementioned data security incident, please do not hesitate to contact me at [mcpaulding@shumaker.com](mailto:mcpaulding@shumaker.com) or directly by telephone at (419) 321-1455.

Very truly yours,

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

Matthew C. Spaulding, Esq.  
Shumaker, Loop & Kendrick LLP

MCS:slo  
Enclosure



## St. John's Jesuit High School & Academy

---

*Men for Others*

August 4, 2020

[NAME]  
[ADDRESS]  
[CITY], [ST] [ZIP CODE]

### **RE: Notice of Data Breach – Important Security and Protection Notification from St. John's Jesuit High School & Academy.**

Dear [Name],

St. John's Jesuit High School and Academy values the relationship we have with our alumni, donors, and friends. We also value your privacy, which is why we are writing to inform you about a recent data security incident involving a third party service provider. This letter contains details about the incident and includes steps you may take to help protect yourself against identity theft.

#### **What Happened?**

On July 16, 2020, St. John's received notice of a ransomware attack suffered by one of our service providers in which a cybercriminal was able to gain access to and begin encrypting certain information on the service provider's systems. St. John's currently utilizes this particular service provider for software and cloud data storage. This service provider hosts our donor database, a legacy database that contains tuition details for students through the 2017-2018 academic year, and they provide us with certain accounting software, which we use to manage vendors and independent contractors. Based on information provided to us by our service provider, it is our understanding that the ransomware attack has been stopped and that they have successfully blocked the cybercriminal's access to the data. After discovering the ransomware attack, our service provider has advised that they contacted law enforcement and engaged independent forensic experts to investigate and help remedy this attack. In connection with that investigation, our service provider has learned that before the cybercriminal's access to the service provider's system was blocked, the cybercriminal was able to successfully remove a copy of their backup file, which contained your personal information. Our service provider has advised that this data security incident occurred at some point beginning on February 7, 2020 and could have continued intermittently until May 20, 2020.

## **Why am I Receiving This Letter?**

Based on St. John's review of the information stored on this service provider's system, you have been identified as either a donor or former student, whose information may have been compromised in the ransomware attack on our service provider.

## **What Information Was Involved?**

Our service provider has informed us that the cybercriminal *did not* have access to any credit card information, bank account information, or social security number. The fields of information that may have been compromised in this data security incident are included below based upon your relationship with St. John's.

### *Donors*

The personal information of donors that may have been compromised in the data security incident includes first and last name, mailing address, email address, business organization name, business mailing address, title, industry, profession, income, date of birth, check number for gifts previously given, and giving history.

### *Former Students*

The personal information of former students that may have been compromised in the data security incident includes first and last name, mailing address, phone number, email address, date of birth, the name of any family members who attended St. John's, tuition amounts charged, any financial aid awarded, and records of payments made (dates and amounts).

## **What Are We Doing?**

Our service provider has advised that based upon the nature of the incident, their own research and third party (including law enforcement) investigation, that they have no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made publicly available. The service provider has advised that they paid the cybercriminal's ransom demand over the data at issue with confirmation that the copy of the data the cybercriminal removed had been destroyed. Nevertheless, we wanted to promptly notify you of this incident to enable you to take immediate action to protect yourself. While our service provider assures us that it has and will continue to implement additional safeguards to prevent future incidents and protect your data, St. John's is currently re-evaluating its relationship with this service provider and the data security standards we require of our service providers.

## **What Can You Do?**

We sincerely regret any inconvenience this data security incident may have caused you. As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. In the event you detect any suspicious activity with an account, you should promptly notify the financial institution or company with which the account



is maintained. You should also promptly report any fraudulent activity or any suspected identity theft to local law enforcement, your state attorney general, and/or the Federal Trade Commission ("FTC"). To file a complaint with the FTC, please visit [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or call (877) ID – THEFT (438-4338).

In addition to the foregoing, we have also enclosed some additional information about obtaining a free credit report and options you may take in connection with guarding against identity theft.

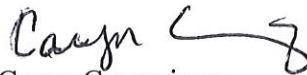
### **More Information**

Should you have any questions or concerns regarding this matter, please do not hesitate to contact us at (419) 865-5743, ext. 0751.

Sincerely,



Michael Savona  
President



Caryn Cummings  
Chief Financial Officer

**ADDITIONAL INFORMATION**  
**YOU HAVE RECEIVED A DATA BREACH NOTICE – STEPS YOU CAN TAKE**

Now that you have been notified that your personal information may have been exposed in a data breach, you should be aware that there are steps you can take to protect yourself from identity theft.

- As a precautionary matter, it is recommended that you remain vigilant and closely monitor your financial account statements and credit reports. Suspicious account activity should be reported to the financial institution or company with which the account is maintained. Any fraudulent activity or suspected identity theft should be promptly reported to law enforcement.
- You may obtain a free copy of your credit report from each of the three major credit reporting agencies on an annual basis (once every 12 months) by visiting <https://www.annualcreditreport.com> and completing and submitting a free credit report request form. Alternatively, you may purchase a copy of your credit report by contacting any one of the three national credit reporting agencies whose contact information for credit report assistance is provided below:

**Equifax**

Automated Service Telephone Number: (800) 685-1111  
Customer Service Telephone Number: (866) 349-5191  
Equifax Information Services LLC  
P.O. Box 740241  
Atlanta, GA 30374-0241  
<https://www.equifax.com>

**Experian**

Telephone Number to Order Credit Report: (888) 397-3742  
Credit Report by mail is unavailable.  
535 Anton Blvd., Suite 100  
Costa Mesa, CA 92626  
<https://www.experian.com>

**TransUnion**

Telephone Number to Order Credit Report: (800) 888-4213  
TransUnion LLC  
P.O. Box 1000  
Chester, PA 19016  
<https://www.transunion.com>

- You may also consider placing a fraud alert on your credit reports with the three major credit reporting agencies. An initial fraud alert will stay on your credit file for at least 90 days. The alert will inform any creditor that makes an inquiry about your credit of possible fraudulent activity and requests that the inquiring creditor contact the individual

prior to establishing any accounts in your name. A fraud alert can be completed by visiting the websites of the credit reporting agencies listed above.

- Additional information about steps you can take to help protect against harm from a data breach, including identity theft, is available online on the Federal Trade Commission (“FTC”) website <https://www.identitytheft.gov>. You can also contact the FTC at (877)-ID-Theft (438-4338) or at:

Identity Theft Clearinghouse  
Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, DC 20580