



St. John's Jesuit High School & Academy

Men for Others

December 18, 2020

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

Subject: **NOTICE OF DATA BREACH (update)**

Dear [INDIVIDUAL NAME]:

We are writing to provide you with an update about the data security incident that we first notified you about back in September of this year. At that time, our service provider had advised St. John's that the data security incident did not include any social security or tax identification numbers. Unfortunately, we have since learned from our service provider that this early assessment was not entirely accurate and that social security and tax identification numbers may have been compromised after all. As a result of these developments and the sensitivity of the information involved, we are writing you again to provide notice of this data breach and to provide you with some additional resources, including free credit monitoring services.

WHAT HAPPENED?

On July 16, 2020, St. John's received notice that one of our service providers had suffered a ransomware attack between February 7, 2020 and May 20, 2020, which involved a cybercriminal gaining access to their system and encrypting a portion of their data. The service provider provides St. John's with software and data storage for our Education Edge software that was used through 2017-2018 school year to store student data and for an Accounts Payable module that we use to manage vendors and independent contractors. Our service provider has informed us that they have rectified the data security incident, but not before the cybercriminal was able to successfully remove a copy of a backup file, which contained some of your information. Our service provider has advised that they paid the cybercriminal's ransom in exchange for confirmation that the backup file had been destroyed.

We are writing you with this correspondence because your information was stored in either the Education Edge database that we used to store student data or our Accounts Payable module that we use to manage vendors and independent contractors.

WHAT INFORMATION WAS INVOLVED?

According to our service provider, the following information may have been compromised from our Education Edge database: first and last name, mailing address, social security number, phone number, date of birth, the name of any family member who attended St. John's, tuition amounts charged, any financial aid award, and records of payments.

Our service provider has also advised that the following information may have been compromised from our Accounts Payable module that we use to manage vendors and independent contractors: vendor name, vendor type, address, customer number, and social security or tax identification.

WHAT WE ARE DOING

As we noted in our earlier communication to you regarding this incident, St. John's values your privacy and deeply regrets that this incident has occurred. We are also disappointed that our service provider did not identify that social security and tax identification numbers may have been compromised before now. St. John's continues to press its service provider for additional details about this data breach incident and we will provide you with updates as appropriate.

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.

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 encourage you to be vigilant in reviewing your credit reports and financial accounts to protect your data and identity.

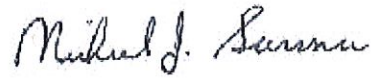
WHAT YOU CAN DO

We encourage you to review the attachment to this letter, which includes important information about actions you may take to further protect your information. We have also included instructions from our service provider for how you may enroll to receive free credit monitoring services to help guard against the threat of identity theft.

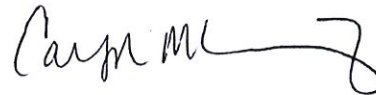
FOR MORE INFORMATION

For further information and assistance, please contact Caryn Cummings at (419) 865-5743, ext. 0751 between the hours of 9:00 a.m. to 5:00 p.m. eastern time.

Sincerely,

A handwritten signature in cursive script, appearing to read "Michael J. Savona".

Michael Savona
President

A handwritten signature in cursive script, appearing to read "Caryn M. Cummings".

Caryn Cummings
Chief Financial Officer

Enclosures

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

As a precautionary measure, St. John's recommends that you remain vigilant by reviewing your account statements and credit reports closely. In the event that you detect any suspicious or unusual activity on an account, you should promptly notify the financial institution or company with whom you maintain the account. You should also promptly report any fraudulent activity or any suspected occurrence of identity theft to the proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). To file a complaint with the FTC, you may visit www.identitytheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. Residents in Rhode Island and Massachusetts also have the right to obtain a police report regarding the data breach incident.

Obtain and Monitor Your Credit Report

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every twelve (12) months by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action> or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax (866) 349-5191 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	Experian (888) 397-3742 www.experian.com P.O. Box 2002 Allen, TX 75013	TransUnion (800) 888-4213 www.transunion.com 2 Baldwin Place P.O. Box 1000 Chester, PA 19016
---	--	---

Consider Placing a Fraud Alert on Your Credit Report

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least ninety (90) days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is also available at <http://www.annualcreditreport.com>.

Credit Freeze

You may also choose to place a security freeze on your credit report, which is a free tool that allows you to restrict access to your credit report, which makes it more difficult for identity thieves to open new accounts in your name because most creditors need to see your credit report before they approve a new account. You may place a freeze on your credit report by contacting each of the nationwide credit bureaus above. You will need to supply your name, address, date of birth, social security number, and prior addresses. After receiving your freeze request, each credit bureau will provide you with a unique personal identification number (PIN) or password. You will need to keep the PIN or password in a safe place because the credit bureau will ask for it when you later request that each temporarily lift or remove the security freeze from your credit report.

For more information about credit freezes and how it differs from a fraud alert, please visit <https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>

Credit Report Monitoring Services

Our third party service provider is providing you with access to Single Bureau Credit Monitoring* services at no charge. Services are for 24 months from the date of enrollment. When changes occur to your Experian credit file, notification is sent to you the same day the change or update takes place with the bureau. In addition, they are providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud you will also have access remediation support from a CyberScout Fraud Investigator. In order for you to receive the monitoring service described above, you must enroll within 90 days from the date of this letter.

Enrollment Instruction

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please navigate to:
<https://www.cyberscouthq.com/epiq263?ac=263HQ1753>

If prompted, please provide the following unique code to gain access to services:
263HQ1753

Once registered, you can access Monitoring Services by selecting the “Use Now” link to fully authenticate your identity and activate your services. **Please ensure you take this step to receive your alerts.**

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

Additional Information

Maryland: Residents of Maryland may also wish to review information made available by the Maryland Attorney General on how to avoid identity theft, at www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, by sending an email to idtheft@oag.state.md.us, by telephone at (410) 528-8662, or via U.S. mail at 200 St. Paul Place, Baltimore, MD 21202.

North Carolina: Residents of North Carolina may obtain more information about preventing identity theft by contacting the North Carolina Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, North Carolina 2799, via telephone at (877) 566-7226 or (919) 716-6000, or online at www.ncdoj.gov.

Rhode Island: Residents of Rhode Island have the ability to file or obtain a police report and may request additional information about identity theft by contacting the Rhode Island, Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, or via telephone at (401) 274-4400.