RE: Notice of Data Breach

Dear (Name),

We are writing to let you know about a data security breach that may have involved your personal information. St. Francis Catholic High School takes the protection and proper use of your personal information very seriously. This letter will explain the incident and provide you with steps you can take to protect yourself.

What Happened
Blackbaud, one of our third-party vendors and one of the world's largest providers of software for nonprofits, university and K12 schools, used by more than 25,000 organizations in more than 60 countries, notified St. Francis of a security breach. Blackbaud stated that its CyberSecurity Team together with forensics experts and law enforcement successfully prevented the cyber criminals from blocking Blackbaud's access. They discovered and stopped the ransomware attack. However, prior to locking the cybercriminal out, it appears a copy of a 2007 backup file containing some of your personal information was removed.

Blackbaud paid the cybercriminal's demand with confirmation the copy removed has been destroyed. Based on the nature of this incident, their research and third party (including law enforcement) investigation, we have no reason to believe any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made available publicly.

Initially Blackbaud assured clients that no personal information had been exposed because it was encrypted. After further investigation, Blackbaud disclosed that some personal information left behind in "legacy" files had not been encrypted.

What Information Was Involved
It is important to note that the cybercriminal did not access your credit card information. However, it has been determined that the file removed may have contained: your daughter's name, date of birth and Social Security number.

What Blackbaud Is Doing
As part of ongoing efforts, Blackbaud states that it already has implemented several changes that will protect your data from any subsequent incidents. First, its teams identified the vulnerability associated with this incident including the tactics used by the cybercriminal, and took action to fix it. Blackbaud has tested its fix with multiple third parties, including the appropriate platform vendors, and assured us that it withstands all known attack tactics. They also are accelerating their efforts to further protect data through enhancements to access management, network segmentation, deployment of additional endpoint, and network-based platforms.

What We Are Doing
We are notifying affected families about this incident. We are continuing to work with Blackbaud to make sure that no sensitive data has been removed from the database. We have no reason to believe the information has been misused or made available publicly but we encourage you to remain vigilant and to report any suspicious activity to law enforcement.

Services

Blackbaud 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, we 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.

Proactive Fraud Assistance. For sensitive breaches focused on customer retention, reputation management, or escalation handling, CyberScout provides unlimited access during the service period to a fraud specialist who will work with enrolled notification recipients on a one-on-one basis, answering any questions or concerns that they may have. Proactive Fraud Assistance includes the following features:

- Fraud specialist-assisted placement of fraud alert, protective registration, or geographical equivalent, in situations where it is warranted.
- After placement of a Fraud Alert, a credit report from each of the three (3) credit bureaus is made available to the notification recipient (United States only).
- Assistance with reading and interpreting credit reports for any possible fraud indicators.
- Removal from credit bureau marketing lists while Fraud Alert is active (United States only).
- Answering any questions individuals may have about fraud.
- Provide individuals with the ability to receive electronic education and alerts through email. (Note that these emails may not be specific to the recipient's jurisdiction/location.)

Identity Theft and Fraud Resolution Services. Resolution services are provided for enrolled notification recipients who fall victim to an identity theft as a result of the applicable breach incident. ID Theft and Fraud Resolution includes, but is not limited to, the following features:

- Unlimited access during the service period to a personal fraud specialist via a toll-free number.
- Creation of Fraud Victim affidavit or geographical equivalent, where applicable.
- Preparation of all documents needed for credit grantor notification, and fraud information removal purposes.
- All phone calls needed for credit grantor notification, and fraud information removal purposes.
- Notification to any relevant government and private agencies.

- Assistance with filing a law enforcement report.
- Comprehensive case file creation for insurance and law enforcement.
- Assistance with enrollment in applicable Identity Theft Passport Programs in states where it is available and in situations where it is warranted (United States only).
- Assistance with placement of credit file freezes in states where it is available and in situations where it is warranted (United States only); this is limited to online-based credit freeze assistance.
- Customer service support for individuals when enrolling in monitoring products, if applicable.
- Assistance with review of credit reports for possible fraudulent activity.
- Unlimited access to educational fraud information and threat alerts. (Note that these emails may not be specific to the recipient's jurisdiction/location.)

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=263HQ1745

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

263HQ1745

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 by **March 27, 2021 at the latest in order to receive this service**.

For More Information
We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have any questions or concerns we did not address in this letter, please contact: ((insert call center information))