



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED

DEC 23 2020

CONSUMER PROTECTION

Paul McGurkin
Office: (267) 930-4788
Fax: (267) 930-4771
Email: pmcgurkin@mullen.law

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

December 15, 2020

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 Saint Francis Ministries ("Saint Francis") located at 110 W. Otis Ave., Salina, KS 67401. In 2019, Saint Francis merged with St. John's Military School ("St. John's") and assumed all rights and responsibilities to former St. John's constituents. We are writing to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident who were formerly affiliated with St. John's. By providing this notice, Saint Francis 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 October 6, 2020, Saint Francis received notification of a cyber incident from one of St. John's former third-party vendors, Blackbaud Inc. ("Blackbaud"). Blackbaud reported that, in May 2020, it experienced a cyber attack incident that resulted in encryption of certain Blackbaud systems. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain customer data stored on its system at some point before Blackbaud locked the cybercriminal out of the system in May 2020. However, only Blackbaud possessed the information necessary to identify the individuals impacted by this event. On November 5, 2020, Blackbaud provided Saint Francis with a list of the impacted individuals and their addresses. Following receipt of this information from Blackbaud, Saint Francis immediately began an investigation to determine the nature and scope of the incident, including what, if any, sensitive Saint Francis data was potentially involved.

Saint Francis confirmed that legally protected personal information may have been present in the involved Blackbaud systems at the time of the incident. The information that could have been subject to unauthorized access includes the names and Social Security number of former St. John's employees.

Notice to New Hampshire Resident

On December 15, 2020, Saint Francis provided written notice of this incident to all affected individuals, which includes one (1) New Hampshire resident. 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

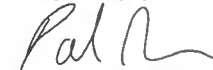
Upon discovering the event, Saint Francis moved quickly to investigate and respond to the incident, assess the security of Saint Francis systems, and notify potentially affected individuals. Saint Francis is providing access to credit monitoring services for one year, through Epiq, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Saint Francis 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. Saint Francis 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4788.

Very truly yours,



Paul McGurkin of
MULLEN COUGHLIN LLC

PTM/slm

EXHIBIT A



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<MailID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Notice of Data Breach

Dear <<Name 1>>:

On October 6, 2020, Saint Francis Ministries ("Saint Francis"), the entity that merged with Saint John's Military School ("St. John's") in 2019, was informed by Blackbaud, Inc. ("Blackbaud"), a third-party vendor who previously provided administrative services to St. John's, that certain Social Security numbers, dates of birth, and bank account information hosted by Blackbaud on behalf of St. John's may have been subject to unauthorized access. This notice provides information about the Blackbaud incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so.

What Happened? Blackbaud reported that, in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to determine the nature and scope of the incident. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that the data was exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. Upon receiving notice of the event from Blackbaud in October 2020, Saint Francis immediately commenced an investigation to determine what, if any, sensitive St. John's data was potentially involved. However, only Blackbaud had access to the list of affected individuals and their addresses. Saint Francis did not receive this information from Blackbaud until November 5, 2020.

What Information Was Involved? Our investigation determined that the involved Blackbaud systems contained your name and <<Data Elements>>. Please note that, to date, we have not received confirmation from Blackbaud that your specific information was accessed or acquired by the unknown actor.

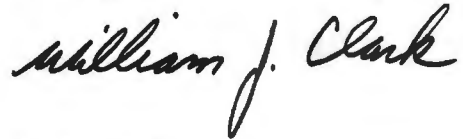
What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities, and we take this incident very seriously. As part of our ongoing commitment to the security of information in our care, we are working to review our existing policies and procedures regarding our third-party vendors, and are working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. We will also be notifying state and federal regulators, as required. We are also offering you twenty-four (24) months of complimentary credit monitoring. Details on how to enroll in this product are included in the enclosed *Steps You Can Take to Help Protect Your Information*.

What You Can Do. We encourage you to enroll in the complimentary credit monitoring we are offering you. We also encourage you to review the enclosed *Steps You Can Take to Help Protect Your Information*. There you will find general information on what you can do to help protect your personal information.

For More Information. We understand that you may have questions about the Blackbaud incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 800-577-9284, 9:00 am to 9:00 pm Eastern Time, Monday through Friday (excluding some U.S. national holidays). You may also write to Saint Francis at 110 W. Otis Ave., Salina, KS 67401.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

A handwritten signature in black ink that reads "William J. Clark". The signature is written in a cursive style with a large, prominent "W" and "C".

William Clark
Interim President, Chief Executive Officer
Saint Francis Ministries, Inc.

Steps You Can Take to Help Protect Your Information

Enroll in Credit Monitoring

As an added precaution, and at no cost to you, we are providing you with access to **Single Bureau Credit Monitoring*** in this matter. Services are for twenty-four (24) months from the date of enrollment. Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services on your behalf. In order for you to receive the monitoring service described above, you must enroll within ninety (90) days from the date of this letter.

To enroll in Credit Monitoring services, please visit: <https://www.cyberscouthq.com> [REDACTED] If prompted, please provide the following unique code to gain access to services: [REDACTED] 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.

ADDITIONAL INFORMATION REGARDING YOUR 24-MONTH MONITORING PRODUCT

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.

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 and comprehensive case file creation for insurance and law enforcement.
- 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.

Monitor Accounts, Financial, and Medical Billing Statements

In general, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five (5) 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, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a one (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 agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. This notice has not been delayed because of a law enforcement request.

The Federal Trade Commission can 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.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

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 agencies 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 Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; and <https://ag.ny.gov/>.

For Oregon residents, the Oregon Attorney General can be reached at: Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096, by phone at (503) 378-4400 and <https://www.doj.state.or.us/oregon-department-of-justice/office-of-the-attorney-general/attorney-general-ellen-f-rosenblum/>. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.