17499

Fay School
[redacted]

FAY SCHOOL

[redacted]

B-87

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

August 6, 2020

Dear [redacted],

I am writing to inform you about a data security incident at Blackbaud, a third-party service provider that may have involved certain information that you provided to Fay School. Fay's Advancement Office uses Blackbaud's Raiser's Edge software application as an engagement and fundraising service, and Blackbaud recently experienced an incident impacting that application. Fay was one of many schools, colleges, and nonprofits that were a part of this incident.

We take the protection and proper use of your information very seriously. Consequently, I am contacting you to explain the incident.

What Happened

On July 16, 2020, Blackbaud notified Fay of a security incident affecting educational institutions and other nonprofits across the United States. Upon learning of the issue, we commenced an immediate and thorough investigation. That investigation is still ongoing. As part of our investigation, in addition to demanding detailed information from Blackbaud about the nature and scope of the incident, we engaged external cybersecurity professionals experienced in handling these types of incidents.

Blackbaud reported to us that as part of an attempted ransomware attack, a backup file containing certain information was removed by the cybercriminal.

What Information Was Involved

We have determined that the compromised file may have contained demographic information and a history of your relationship with Fay, such as donation dates and amounts. The cybercriminal did not access your credit card or social security number information because Fay does not store this information in the database.

Unfortunately, copies of some donation checks that were written to Fay between June 2011 and May 2020 appear to have been part of the compromised file. Consequently, we learned on July 23, 2020 that it is possible that the cybercriminal may have gained access to your bank account information, specifically your name, address, bank routing number, checking account number, and signature.

Based on the nature of the incident, the research performed by Blackbaud, and third-party investigators, Blackbaud has told us there is no reason to believe that any data went beyond the cybercriminal, was or will be misused, or will be disseminated or otherwise made available publicly. Blackbaud indicates that it has hired a third-party team of experts, including a team of forensic accountants, to continue monitoring for any such activity.

What Our Service Provider Is Doing

According to Blackbaud, they quickly identified the vulnerability associated with this incident, including the methods used by the cybercriminal, and immediately responded to and resolved the issue. They report that they were able to successfully stop the attack and close the vulnerability, and that they confirmed this with thorough testing through multiple third parties and security experts. Blackbaud has assured Fay that they are enhancing their security controls and conducting ongoing efforts against incidents like this in the future, and that they have already implemented several changes that will protect your data.

What We Are Doing and What You Can Do

We have been deeply troubled by this incident. We are always assessing and reviewing our own internal policies and procedures to protect against the evolving nature of cyber crime. We are also taking active steps to improve our processes in the Advancement Office so we can better protect the privacy of our donors' information.

We urge you to remain vigilant and promptly report to the proper law enforcement authorities any suspicious activity, irregularities in your bank accounts, or suspected identity theft. Because your checking account number may have been compromised, we recommend that you contact your financial institution to discuss ways in which you can best protect your account, including changing your account number. This letter also includes precautionary measures you can take to protect your personal information, including by placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. We will update you, as appropriate, if we learn more from the forensic accountants who are investigating this incident or from Blackbaud generally about the scope of this incident.

For More Information

If you have questions about which of your checks may have been part of this incident, please contact me directly at [redacted].

I deeply apologize for this situation and regret any inconvenience it may cause you. Fay's relationship with you, and with all of our donors, is essential to the School's success, and we appreciate how important it is to retain your trust. I would be happy to speak with you directly to discuss this incident further, and I thank you once again for your loyalty and dedication to Fay.

Sincerely,

[redacted]

[redacted]

[redacted]

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial 1-year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	**Experian**	**TransUnion LLC**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

2. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing or by mail, to all three nationwide credit reporting companies. To find out more about how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	**ExperianSecurity Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/securityfreeze
1-800-685-1111	1-888-397-3742	1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit monitoring company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. **Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

5. **Obtaining a Police Report.**

Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.