FAQs for Blackbaud Data Incident - Banking Parent Letter

Q: Why did I receive a message about Blackbaud from St. Francis Catholic High School?

A: St. Francis Catholic High School contracts with Blackbaud, one of the world's largest providers of software from nonprofit organizations, universities and K12 schools. Information is stored in a private, cloud-based environment provided by Blackbaud. In July 2020, SFHS was notified about a ransomware attack that occurred at Blackbaud but we were not identified as being affected at that time. After extensive third-party audits in the fall of 2020, Blackbaud informed St. Francis that their conversion data file containing student information may have been compromised. SFHS conducted an exhaustive search to verify those individuals impacted.

Q: What information was involved in this data security incident at Blackbaud?

A: The specific information that was involved should be addressed in the letter you received. It has been determined that the file removed may have contained: student name, date of birth, parent/guardian name and bank account number from 2005 to 2007.

Q: What is St. Francis Catholic High School and Blackbaud doing to address the situation?

A: St. Francis and Blackbaud are working together to distribute any new information about the data security breach. Blackbaud has already implemented and tested additional security measures to protect your data from any subsequent incidents. While data breaches and ransomware attacks are becoming more common, this is not an issue St. Francis every wants to happen to our families and supporters. We take your privacy seriously, and we will continue to work with Blackbaud and law enforcement to monitor this incident. We regret any inconvenience it may cause.

Q: What should I do?

A: We recommend, as a best practice, to continue monitoring your personal information online and report any suspicious activity to your financial institution and/or the appropriate authorities.

Q: Are you providing credit monitoring services?

A: No, we are not providing credit monitoring services since your social security number was not affected.

The Federal Reserve has noted that payments fraud involving the use of Automated Clearing House information, or ACH, remains rare due largely to the technological innovations banks and payment providers have put in place to identify and mitigate fraud at the point where funds are dispersed and deposited. In many cases access to an account number will only allow the person who has the account's number to transfer money to that account. It is true there are cases when it becomes possible to set up a

direct debit to a vendor, however most banks require verification signatures to set up a direct debit. Additionally, banks have protection systems designed to monitor suspicious activities on their customers' accounts. Blackbaud has no reason to believe that any data went beyond the cybercriminal, or will be misused, or will be disseminated or otherwise made available publicly. Blackbaud paid the cybercriminal's ransom demand with confirmation they deleted the information and engaged in a 3rd party which is conducting ongoing monitoring of the dark web. There is no evidence it is being made available publicly. In the unlikely event that were to happen, we will notify you. If you have additional concerns, some general best practice actions you can take are the following:

1. Examine bank account activity daily and reconcile bank accounts regularly
2. Utilize your bank's debit block features to ensure unauthorized debits cannot be made on your bank accounts so you can pre-authorize any account debits
3. Confirm any requests via email to change a vendor's bank account with an actual call back to the vendor

You can also obtain a copy of your credit report, free of charge, from the three nationwide credit reporting companies. To do this, you can visit www.annualcreditreport.com, call toll free at 1-877-322-8228, or directly contact the three nationwide credit reporting companies:

Equifax	Experian	TransUnion
PO Box 740241	PO Box 9554	PO Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

Q: What are you doing to protect the continued security of my information?

A: Blackbaud 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.