



Dear MCLA Community:

We are emailing to let you know about a data incident that we were made aware of by one of our vendors, Blackbaud. Blackbaud is a cloud database and fundraising management tool that provides services to many university foundations and nonprofit organizations.

On July 16, 2020, Blackbaud notified us, as well as hundreds of other organizations that use its services, that it was impacted by a ransomware event. According to Blackbaud, in May 2020, ransomware was deployed within Blackbaud's environment and some of its data was exfiltrated out of its systems. Blackbaud encrypts most of the data it stores, but some of the less sensitive fields are left unencrypted. According to Blackbaud, information such as Social Security numbers, payment card data, and financial account information was not impacted. Blackbaud's explanation of the incident can be found here: <https://www.blackbaud.com/securityincident>

Unfortunately, the Massachusetts College of Liberal Arts Foundation was one of the organizations whose information was impacted. We are frustrated with the way in which Blackbaud has handled this matter, but continue to work with them to acquire additional information about the incident and confirm that there is a low risk to our constituents' information. We are also reviewing our relationship with Blackbaud.

We value the trust you place in us and take our responsibility to safeguard your personal information seriously. We apologize for any inconvenience or concern this incident may cause. Once our investigation is complete, if we find out additional relevant information, we will send follow-up communications to individuals whose sensitive personal information may have been impacted. In the meantime, if you have any questions, please contact [advancement@mcla.edu](mailto:advancement@mcla.edu) or simply reply to this email.

Sincerely,

A handwritten signature in black ink, appearing to read 'Robert P. Ziomek', located below the 'Sincerely,' text.

Robert P. Ziomek  
President  
MCLA Foundation, Inc.

## **Frequently Asked Questions**

**Q. What happened?**

A. On July 16, 2020, Blackbaud one of our vendors, notified us, as well as hundreds of other organizations that use its products, that that it was impacted by a ransomware event. Blackbaud is a cloud database and fundraising management tool that provides services to many university foundations and organizations. According to Blackbaud, in May 2020, ransomware was deployed within Blackbaud’s environment and some of the data it was storing on behalf of its customers was exfiltrated out of its systems. Blackbaud encrypts most of the data it stores, but some of the less sensitive fields are left unencrypted. As a result, some fields such as individuals’ names, dates of birth, and giving history, may have been accessible to the bad actor. According to Blackbaud, information such as Social Security numbers, payment card data, and financial account information was not impacted.

Unfortunately, the Massachusetts College of Liberal Arts Foundation was one of the organizations whose information was impacted. We are frankly frustrated with the way in which Blackbaud has handled this matter, but are working with them to get additional information about the incident and confirm that there is a low risk to our constituents’ information. We are also reviewing our relationship with Blackbaud.

Our investigation is ongoing but, once it is complete, if we find out additional relevant information, we will communicate with individuals whose sensitive personal information may have been impacted.

**Q. When did this happen, and when did you learn about it?**

A. According to Blackbaud, the incident occurred in May 2020. Blackbaud notified us on July 16, 2020.

**Q. What are you going to do to prevent this from happening again? What security protections have you put in place to better protect information following this incident?**

A. We take this matter seriously and are reviewing our relationship with Blackbaud. If our relationship with Blackbaud will continue, we will review their security protocols before moving forward with their services.

**Q. Who did this?**

A. We do not know the identity of the individual or individuals responsible for this incident.

**Q. Why was I notified?**

A. We take the privacy and confidentiality of the information you entrusted to us seriously. Although our investigation is ongoing, we wanted to let you know that this has happened as soon as possible.

**Q. Am I affected? I am an alumni of the College and heard about a breach but did not receive a letter. Why not?**

A. Based on our investigation so far, the information that was impacted was very minimal. We have notified all potentially impacted individuals of the situation and will follow up with formal breach notification letters to anyone whose sensitive personal information was impacted.

**Q. Why wasn't I contacted sooner?**

A. While the incident occurred in May 2020, we first heard about it from Blackbaud on July 16, 2020. Frankly we are frustrated that it took Blackbaud so long to let us know. Upon learning of the incident we immediately started investigating what happened. Our investigation is still ongoing but we wanted to let our community know about the incident as soon as possible.

**Q. What specific information may have been compromised?**

A. According to Blackbaud, most of the information in the system was encrypted prior to the ransomware attack, and so would not have been accessible to the bad actor. Our understanding is that the information that was at risk includes individuals' names, demographic and contact information, dates of birth, and giving history.

**Q. Are the rest of the organization's computer systems secure?**

A. Yes, this incident involves Blackbaud and does not impact any of the College's systems.

**Q. How will I know if my information was used by someone else?**

At this point, we have no reason to believe that your information has been used to commit fraud or identity theft. Blackbaud has provided additional information about this incident, as well as information people can use to protect themselves. We recommend visiting the website they setup, which is <https://www.blackbaud.com/securityincident>.