

August 7, 2020

TO: UCF Advancement Vendors
FROM: Mike Morsberger
RE: Blackbaud Server Data Breach

Recently, we were notified by Blackbaud, a company that provides cloud-based computing software to nonprofits, educational institutions and others, that UCF Foundation accounting data hosted on Blackbaud's servers was breached in a ransomware attack. No donor biographical information was compromised, as that data is not stored in this program. While UCF Foundation vendor data was involved, all sensitive information was encrypted to safeguard against events such as this.

Because the UCF Foundation had only recently transitioned to Blackbaud's cloud-based accounting software, only information limited to this system was involved.

Blackbaud was successful in expelling the cybercriminal from its system and continues to work with forensic experts and law enforcement to address this issue. The UCF Foundation reviewed the data involved and determined no sensitive information was compromised. Vendor information in the breach included publicly available data such as names of businesses or individuals with whom UCF Advancement conducted business and, in some cases, addresses, emails and phone numbers. No social security numbers, driver's license information, passwords or other confidential data was accessed, therefore, no action is needed on your part.

Data security is of the utmost importance to the UCF Foundation, and data encryption is just one of many safeguards used to prevent sensitive information from being compromised. To read more about this incident, please visit <https://www.blackbaud.com/securityincident>

If you have questions about the data breach, please contact Dan Lopresto, Director of Privacy Compliance, at Daniel.lopresto@ucf.edu.

Mike Morsberger
Vice President, University Advancement