



Dear Urban Community,

We recently received a notification from Blackbaud, a widely used software service provider for schools, colleges and other non-profits, including Urban, that its server was subject to a ransomware attack in May 2020. Blackbaud has informed us that its security team was able to successfully block and expel the cybercriminals from their system, and that the cybercriminal did NOT access credit or debit card information, bank account information, usernames, passwords or Social Security numbers.

However, Blackbaud acknowledged that before being expelled, the cybercriminals accessed a subset of data that may have included some information on the school community, including names, addresses, payment and fundraising history. After discovering the attack, Blackbaud's Cyber Security team—together with independent forensics experts and law enforcement—paid a ransom for confirmation that this subset of data was permanently destroyed, and reported to us that, **"based on the nature of the incident, our research, and third party (including law enforcement) investigation, we have 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."** In spite of this reassurance, we felt it important to reach out to let you know and to stress how seriously we take any threat to our data security or the confidential information shared with the school.

[This link](#) from *The NonProfit Times* offers more details about the incident, as does the [official statement](#) from Blackbaud.

If you have questions or concerns, please feel free to contact us at cybersecurity@urbanschool.org.

Sincerely,

Igor Zagatsky
Director of Information Services

Diane Walters
Chief Financial Officer