As alumni and supporters of the Metropolitan State University Foundation, we want you to know about an incident that may have involved your personal contact information. In July, we were notified by Blackbaud, a company that provides Metro State Foundation with data management and software services, that they had experienced a data security incident. You may have already received a notification about this incident from other nonprofits you support, as Blackbaud's fundraising and database services are used by thousands of nonprofit organizations worldwide and 15 of the 37 institutions of higher education in the Minnesota State System.

What's Important to Know
No credit card, bank account, or other unique and sensitive information, such as social security number, was compromised.

What Happened
Blackbaud was the target of a ransomware attack sometime between February 7, 2020, and intermittently until May 20, 2020. The hackers attempted to disrupt business by locking users out of their own data and in the process, accessed personally identifying information about Blackbaud's nonprofit clients, including those of the Metro State Foundation. Blackbaud informed us of the breach on July 16, 2020.

After discovering the attack in May 2020, Blackbaud's Cyber Security team—together with independent forensics experts and law enforcement—retrieved the stolen data and successfully prevented the cybercriminal from blocking their system access and fully encrypting files, and ultimately expelled them from the system.

The Minn State system IT and legal team launched an independent investigation on July 16 and sent us their confirmation of Blackbaud's findings. We took the time to verify Blackbaud's findings through the independent investigation before sending this message to our supporters.

What Information Was Involved
Metropolitan State University Foundation ***does not*** store social security numbers or any banking account information within the Blackbaud system. Therefore, we can confirm that your social security number, credit card or bank account information were not breached. However, it is possible that contact information for some individuals may have been compromised. The information obtained by the intruders could include: name, address, phone number, email address, and if applicable, date of birth.

Blackbaud believes they have addressed this incident and are taking steps to ensure its security system is not compromised again. A full description of the incident is available on the Blackbaud site at: https://www.blackbaud.com/securityincident.

What We Are Doing
We sincerely apologize for this incident and regret any inconvenience it may cause. We take data security very seriously, along with the trust you place in us. We are confident in Metropolitan State University Foundation's internal data security and

privacy practices and will continue to work with Blackbaud to ensure your privacy and security is not compromised.

What You Can Do
As a best practice, we recommend you remain vigilant and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities such as the Federal Trade Commission, and the Office of the Minnesota State Attorney General.

Contact Us
If you have questions, concerns or would like specific information about your personal data please contact Missi Worthington, Prospect Development Manager via email at melissa.worthington@metrostate.edu.