UNIVERSITY OF
St.Thomas

All for the Common Good™

August 14, 2020

VIA CERTIFIED MAIL AND EMAIL AT NDAG@ND.GOV

Office of the Attorney General
Consumer Protection & Antitrust Division
600 E. Boulevard Avenue Dept. 125
Bismarck, ND 58505

Re: Notice of Data Incident

Dear Attorney General Stenehjem:

We are writing to notify you of a recent information management service provider's data incident that involved personal information of North Dakota residents.

On July 16, 2020, Blackbaud, Inc. (Blackbaud) notified the University of St. Thomas (St. Thomas) that on May 14, 2020, Blackbaud discovered a ransomware attack that involved information maintained for St. Thomas in ResearchPoint. A cybercriminal removed a backup copy of our data in ResearchPoint from Blackbaud's self-hosted storage environment. According to Blackbaud, this incident occurred between February 7, 2020 and May 20, 2020.

When Blackbaud became aware of this incident, it took steps, together with independent forensics experts and law enforcement, to prevent the cybercriminal from blocking Blackbaud's system access and fully encrypting files, and ultimately expelled the cybercriminal from Blackbaud's system. Blackbaud paid the cybercriminal's ransom demand with confirmation that the copy removed by the cybercriminal had been destroyed.

Blackbaud confirmed that that none of our data was lost or corrupted as a result of this incident.

Some or all of the following St. Thomas database information about the university's supporters and friends may have been involved in this incident: name, spouse's name, postal address, telephone number, email address, St. Thomas student identification number, date of birth, and information about the individual's relationship with us.

The St. Thomas data did **not** contain any credit card information, bank account information, usernames, passwords or Social Security Numbers, and Blackbaud has confirmed that the copy removed by the cybercriminal did not contain any credit card information and the cybercriminal did not gain access to bank account information, usernames, passwords, or Social Security Numbers.

We have been working with Blackbaud to enhance our understanding about this incident and Blackbaud's data security and to help prevent a similar incident from occurring in the future. Blackbaud notified us that it has implemented changes so that such an incident does not happen again.

Blackbaud said that based on the nature of this incident, Blackbaud's research, and investigations conducted by third parties including law enforcement, Blackbaud has 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. Blackbaud also has retained a third-party team of experts to monitor the dark web as an extra precautionary measure.

The names and dates of birth of 751 North Dakota residents were involved in this incident. We are preparing notifications to send to these North Dakota residents starting on or about August 14, 2020 to inform them of this incident. These notifications will be sent by mail or email and copies of the forms of notification letter and email notification are enclosed. We also are posting information about the incident on our website and providing notice to major statewide media. Substitute notice is appropriate because we do not have sufficient contact information to provide notification letters by mail to all North Dakota residents.

If you have any questions, please contact me at (651) 962-6511 or gros6968@stthomas.edu.

Sincerely,

Sara Gross Methner
General Counsel & Secretary

Enclosures

FORM OF NOTIFICATION LETTER

August 14, 2020

<<Name>>
<<Address>>

Dear <<Name>>:

We value our relationship with you and are writing to inform you about an incident that involved personal information about you.

WHAT HAPPENED

Blackbaud, Inc. (Blackbaud) provides certain information management services to us through a product called ResearchPoint. On July 16, 2020, Blackbaud notified us that on May 14, 2020, Blackbaud discovered a ransomware attack that involved information maintained for the University of St. Thomas in ResearchPoint. A cybercriminal removed a backup copy of our data in ResearchPoint from Blackbaud's self-hosted storage environment. According to Blackbaud, this incident occurred between February 7, 2020 and May 20, 2020.

When Blackbaud became aware of this incident, it took steps, together with independent forensics experts and law enforcement, to prevent the cybercriminal from blocking Blackbaud's system access and fully encrypting files, and ultimately expelled the cybercriminal from Blackbaud's system. Blackbaud paid the cybercriminal's ransom demand with confirmation that the copy removed by the cybercriminal had been destroyed.

Blackbaud confirmed that that none of our data was lost or corrupted as a result of this incident.

WHAT INFORMATION WAS INVOLVED

This incident involved our data in ResearchPoint, which includes certain information about St. Thomas supporters and friends. Some or all of the following information may have been involved in this incident: your name, spouse's name, postal address, telephone number, email address, St. Thomas student identification number (if applicable), date of birth, and information about your relationship with us.

The data did **not** contain any credit card information, bank account information, usernames, passwords or Social Security Numbers, and Blackbaud has confirmed that the copy removed by the cybercriminal did not contain any credit card information and the cybercriminal did not gain access to bank account information, usernames, passwords, or Social Security Numbers.

WHAT WE ARE DOING

We have been working with Blackbaud to enhance our understanding about this incident and Blackbaud's data security and to help prevent a similar incident from occurring in the future. Blackbaud notified us that it has implemented changes so that such an incident does not happen again.

Blackbaud said that based on the nature of this incident, Blackbaud's research, and investigations conducted by third parties including law enforcement, Blackbaud has 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. Blackbaud also has retained a third-party team of experts to monitor the dark web as an extra precautionary measure.

WHAT YOU CAN DO

While no credit card or payment data was involved in this incident, we encourage you to always closely review your payment card statements for any unauthorized charges. Immediately report any unauthorized charges to the bank that issued your card, as payment card network rules generally provide cardholders are not responsible for unauthorized charges when timely reported.

FOR MORE INFORMATION

We regret that this incident occurred and sincerely apologize for any inconvenience this may have caused. If you have any questions, please contact us at (651) 962-6950 or development@stthomas.edu.

Sincerely,

Erik Thurman
Vice President for University Advancement
University of St. Thomas

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity.

You may obtain a copy of your credit report, free of charge, once every twelve months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- Experian, PO Box 2002, Allen, TX 75013, www.experian.com,1-888-397-3742
- TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

You may also consider contacting the three nationwide credit reporting companies directly if you wish to obtain information about fraud alerts and security freezes.

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

Contact information for the Federal Trade Commission is as follows:

- Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, IdentityTheft.gov, 1-877-ID-THEFT (438-4338)

To obtain information about fraud alerts, visit https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

To obtain information about security freezes, visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

FORM OF EMAIL NOTIFICATION

Subject: Notice of Data Incident

August 14, 2020

Dear <<Name>>:

We value our relationship with you and are writing to inform you about an incident that involved personal information about you.

WHAT HAPPENED

Blackbaud, Inc. (Blackbaud) provides certain information management services to us through a product called ResearchPoint. On July 16, 2020, Blackbaud notified us that on May 14, 2020, Blackbaud discovered a ransomware attack that involved information maintained for the University of St. Thomas in ResearchPoint. A cybercriminal removed a backup copy of our data in ResearchPoint from Blackbaud's self-hosted storage environment. According to Blackbaud, this incident occurred between February 7, 2020 and May 20, 2020.

When Blackbaud became aware of this incident, it took steps, together with independent forensics experts and law enforcement, to prevent the cybercriminal from blocking Blackbaud's system access and fully encrypting files, and ultimately expelled the cybercriminal from Blackbaud's system. Blackbaud paid the cybercriminal's ransom demand with confirmation that the copy removed by the cybercriminal had been destroyed.

Blackbaud confirmed that that none of our data was lost or corrupted as a result of this incident.

WHAT INFORMATION WAS INVOLVED

This incident involved our data in ResearchPoint, which includes certain information about St. Thomas supporters and friends. Some or all of the following information may have been involved in this incident: your name, spouse's name, postal address, telephone number, email address, St. Thomas student identification number (if applicable), date of birth, and information about your relationship with us.

The data did **not** contain any credit card information, bank account information, usernames, passwords or Social Security Numbers, and Blackbaud has confirmed that the copy removed by the cybercriminal did not contain any credit card information and the cybercriminal did not gain access to bank account information, usernames, passwords, or Social Security Numbers.

WHAT WE ARE DOING

We have been working with Blackbaud to enhance our understanding about this incident and Blackbaud's data security and to help prevent a similar incident from occurring in the future. Blackbaud notified us that it has implemented changes so that such an incident does not happen again.

Blackbaud said that based on the nature of this incident, Blackbaud's research, and investigations conducted by third parties including law enforcement, Blackbaud has 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. Blackbaud also has retained a third-party team of experts to monitor the dark web as an extra precautionary measure.

WHAT YOU CAN DO

While no credit card or payment data was involved in this incident, we encourage you to always closely review your payment card statements for any unauthorized charges. Immediately report any unauthorized charges to the bank that issued your card, as payment card network rules generally provide cardholders are not responsible for unauthorized charges when timely reported.

FOR MORE INFORMATION

We regret that this incident occurred and sincerely apologize for any inconvenience this may have caused. If you have any questions, please contact us at (651) 962-6950 or development@stthomas.edu.

Sincerely,

Erik Thurman
Vice President for University Advancement
University of St. Thomas

***

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity.

You may obtain a copy of your credit report, free of charge, once every twelve months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- Experian, PO Box 2002, Allen, TX 75013, www.experian.com,1-888-397-3742
- TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

You may also consider contacting the three nationwide credit reporting companies directly if you wish to obtain information about fraud alerts and security freezes.

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about

fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

Contact information for the Federal Trade Commission is as follows:

- Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, IdentityTheft.gov, 1-877-ID-THEFT (438-4338)

To obtain information about fraud alerts, visit https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

To obtain information about security freezes, visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.