NOTICE TO DONORS

The Archdiocese recently received information from Blackbaud, the third-party service provider for Archdiocesan electronic gifts and donor management. Blackbaud is one of the world's largest providers of customer relationship management software. Blackbaud was subject to a data security incident known as a "ransomware attack." The security incident may have involved information maintained by the Archdiocese of Dubuque.

Blackbaud has conducted an appropriate investigation, in conjunction with law enforcement officials. After an investigation of our own, the best available information indicates that there is no reasonable likelihood of financial harm to any person whose personal information could have been acquired through the Archdiocese of Dubuque in the security breach. Even though additional notices in circumstances such as these are not necessary, both Blackbaud and the Archdiocese of Dubuque have erred on the side of caution in sharing the following additional details to increase awareness and to encourage diligence in monitoring any suspicious activity.

Blackbaud reported that the data security incident started on February 7, 2020 and possibly continued intermittently until May 20, 2020. The Archdiocese of Dubuque was one of numerous organizations that was impacted. We were notified on July 16 of this situation.

Blackbaud assured us that no data such as Social Security numbers, bank account information, and credit and debit card information was accessible because they were encrypted. We are continuing with our internal investigation to confirm this assurance. If any such data is found to have been viewable, we will notify the impacted individuals directly.

According to Blackbaud, the sophisticated cyber-attack was successfully stopped, and the cybercriminals were expelled from its system. However, Blackbaud informed us that the cybercriminals did remove a copy of a backup file stored as part of Blackbaud's normal operations. We believe that the backup file ***may have*** contained limited non-financial information for some of our supporters, such as contact information, date of birth, limited demographic data and a history of gifts to the Archdiocese, Our Faith STO, Catholic Charities and the Catholic Foundation in the Archdiocese (CFAD). But again, this backup file ***would not have*** included social security numbers, driver's license numbers, unique identification numbers by a government body, financial account numbers, credit card numbers, or debit card numbers in combination with any required expiration date, security code, access code, or password that would permit access to an individual's financial account, any unique electronic identifier or routing code in combination with any required security code, access code, or password that would permit access to an individual's financial account, or unique biometric data.

Blackbaud further assured us that, based on the nature of the incident, their research, and law enforcement's investigation, the stolen data has been

destroyed and there is no reason to believe any data went beyond the cybercriminals, was or will be misused, or will be disseminated or otherwise made available publicly. In addition, Blackbaud has engaged a third-party team of experts to monitor the dark web as an extra precautionary measure.

Based on the above, we do not believe there is a need for you to take any action at this time. As a best practice, we recommend that you remain vigilant and promptly report any suspicious activity or suspected identity theft to the proper authorities, including local law enforcement or the Iowa Attorney General's Office (515-281-5926//888-777-4590 (outside of the Des Moines metro area)), or you may contact one of the following national consumer reporting agencies:

Equifax

Online: www.ai.equifax.com/CreditInvestigation
By mail: Click here to download the dispute form
Mail the dispute form with your letter to:
Equifax Information Services LLC
P.O. Box 740256
Atlanta, GA 30374
By phone: Phone number provided on credit report or (800) 864-2978

Experian

Online: www.experian.com/disputes/main.html
By mail: Use the address provided on your credit report or mail your letter to:
Experian
P.O. Box 4500
Allen, TX 75013
By phone: Phone number provided on credit report or (888) 397-3742

TransUnion

Online: www.transunion.com/personal-credit/credit-disputes-alerts-freezes.page
By mail: Click here to download the dispute form
Mail the dispute form with your letter to:
TransUnion LLC
Consumer Dispute Center
P.O. Box 2000
Chester, PA 19016
By phone: (800) 916-8800

We value your relationship with us and the faith you put in us. Please know that we take the security of your information very seriously and share your concern about this incident. Blackbaud has already implemented changes to its security controls to better protect against a potential future attack, and we are working with Blackbaud to assess the best path forward.

While the Archdiocese was not the target of this attack, nor was it the only organization affected, we are taking time to learn from this third-party incident and to review our own security practices and system configurations to protect your information even better.

Thanks to each of you for your continued support of the important mission of the Church.

Sincerely,

Jeff Henderson
Director of Stewardship Development
563-556-2580 ext. 307