M. Alexandra Belton
Office: (267) 930-4773
Fax: (267) 930-4771
Email: abelton@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

August 31, 2020

VIA E-MAIL

Office of the Attorney General
Consumer Protection and Antitrust
Gateway Professional Center
1050 E Interstate Avenue Suite 200
Bismarck, ND 58503-5574
E-mail: ndag@nd.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent American Bible Society ("ABS") located at North Independence Mall, 101 East FL8, Philadelphia, PA 19106 and write to notify your Office of an incident that may affect the security of some personal information relating to four thousand two hundred seventy (4,270) North Dakota residents. This notice may be supplemented if any new significant facts are learned subsequent to its submission. By providing this notice, ABS does not waive any rights or defenses regarding the applicability of North Dakota law, the applicability of the North Dakota data event notification statute, or personal jurisdiction.

Nature of the Data Event

On July 16, 2020, ABS received a communication from one of its third-party vendors, Blackbaud, Inc. ("Blackbaud"), of a cyber incident. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to organizations, including ABS. Upon receiving notice of the cyber incident, ABS immediately commenced an investigation to better understand the nature and scope of the incident and any impact on ABS data. This investigation included working diligently to gather information from Blackbaud to understand the scope of the incident. On August 5, 2020, ABS received further information from Blackbaud that allowed it to confirm the information potentially affected may have contained personal information.

In its initial communication, Blackbaud reported that, in May 2020, it experienced a ransomware incident that resulted in encryption of certain Blackbaud systems. Blackbaud reported the incident to law enforcement and worked with forensic investigators to determine what occurred. Following its investigation, Blackbaud notified its customers that an unknown actor may have accessed or acquired certain Blackbaud customer data. Blackbaud reported that the data was exfiltrated by the threat actor at some point before Blackbaud locked the threat actor out of the environment on May 20, 2020. Based on ABS' investigation, it was determined that the information that could have been subject to unauthorized acquisition includes name and date of birth.

Notice to North Dakota Residents

On or about August 31, 2020, ABS provided written notice of this incident to affected individuals, which include four thousand two hundred seventy (4,270) North Dakota residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, ABS moved quickly to investigate and respond to the incident and to notify potentially affected individuals. This included extensive coordination with Blackbaud to confirm what information could have been potentially affected that may have contained personal information. ABS is working to review existing policies and procedures regarding third-party vendors and is working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future.

Additionally, ABS is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. ABS is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. ABS will also be notifying other state regulators as required.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4773

Very truly yours,

M. Alexandra Belton of
MULLEN COUGHLIN LLC

EXHIBIT A

AMERICAN BIBLE SOCIETY

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

On July 16, 2020, American Bible Society received notice from Blackbaud, our data service provider, of a cybersecurity event that occurred on their systems that was discovered in May of 2020. Blackbaud is a data service provider supporting mainly nonprofit organizations, such as ours, educational institutions and more.

This cyberattack included unauthorized access to data Blackbaud holds on our behalf, including personal information of our donors. Blackbaud has assured us, however, that social security, credit card and bank account information were not compromised, because that data, to the extent it is held by Blackbaud, is encrypted and stored on a server not subject to this breach. Blackbaud also has assured us that it has taken extensive steps to reduce the risk of this cyberattack to our donors and to reduce the risk of similar attacks in the future, including paying the cyber criminals to delete the data that was taken and to monitor the Internet "dark web" to confirm that the data is not sold or distributed to others.

On August 5, 2020, American Bible Society received further information from Blackbaud that allowed us to determine the information potentially affected may have contained personal information. While Blackbaud has not confirmed that your information specifically was included in data that was acquired by the unknown actor, we are notifying you out of an abundance of caution because your name and date of birth were located in the backup file of American Bible Society.

We take the confidentiality, privacy, and security of personal information very seriously. American Bible Society has security measures in place to protect information in our care.

Based on our independent investigation and the information provided to us by Blackbaud, we believe the risk of this incident to our donors is low. Nonetheless, because we value our relationship with you, we are letting you know all of this in the interest of transparency and in consideration of your support of our organization.

As a best practice, we recommend you remain vigilant and promptly report any suspicious activity to the proper law enforcement authorities. In addition, we are providing you with useful resources and suggestions in the following "Recommendations for Protecting Personal Information".

We will continue to work with Blackbaud to further investigate this matter. Should you have any questions or concerns regarding this matter, please do not hesitate to contact us at datacare@americanbible.org or by phone at 1-???-???-???? Monday through Friday 9:00 am to 6:30 pm Eastern Time.

We are thankful for your continued support and engagement.

Blessings,

John Clause
Senior Vice President
American Bible Society

Stephen S. Kao
General Legal Counsel
American Bible Society

RECOMMENDATIONS FOR SAFEGUARDING PERSONAL INFORMATION

We encourage you to remain vigilant against incidents of identity theft and fraud. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	TransUnion	Equifax
P.O. Box 9554	P.O. Box 2000	P.O. Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	TransUnion	Equifax
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), and TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint. You can obtain further information on how to file such a complaint by way of the contact information provided above. In addition, you have the right to file a police report if you ever experience identity theft or fraud. Please note that to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim.