MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Alexander T. Walker
Office: (267) 930-4801
Fax: (267) 930-4771
Email: awalker@mullen.law

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

November 24, 2020

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Friends Seminary located at 222 East 16th Street, New York, NY 10003, and are writing to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident, which was made known to Friends Seminary by its third-party vendor, Blackbaud, Inc. ("Blackbaud"). The investigation into this matter, and the impact on Friends Seminary is ongoing. Accordingly, this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Friends Seminary does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On Thursday, July 16, 2020, one of Friends Seminary's vendors, Blackbaud, informed Friends Seminary that it suffered a ransomware attack that resulted in potential unauthorized access to certain information maintained by its systems, but that it did not have any indication that Social Security numbers or financial account information was at risk. On October 5, 2020, Friends Seminary was further notified by Blackbaud that Social Security numbers, bank account information and other payroll information were, in fact, present in a payroll table from a legacy version of the financial services tool which remained after conversion to a new tool and therefore were at risk for unauthorized access due to the same incident originally reported in July.

The information that could have been subject to unauthorized access includes name, address, Social Security numbers and financial account information. Although Friends Seminary has already identified its current employees impacted by this issue and provided written notification to them on November 24, 2020, as detailed further below, a review of all impacted personal information for former

employees and possibly other types of individuals is ongoing to determine if further notifications are to be made.

Notice to New Hampshire Resident

On or about November 12, 2020, Friends Seminary provided written notice of this incident via email to affected current employees, which includes one (1) New Hampshire resident. This email notice was provided in substantially the same form as the content attached here as ***Exhibit A***. Additionally, written notice was mailed to these same affected current employees on November 24, 2020, in substantially similar form to the content attached hereto as ***Exhibit B***.

Other Steps Taken and To Be Taken

Upon discovering the event, Friends Seminary moved quickly to investigate and respond to the incident, assess the security of Friends Seminary systems, and notify potentially affected individuals. Friends Seminary is also working to review existing policies and procedures regarding third-party vendors and are working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. Friends Seminary is providing access to credit monitoring services for two (2) years through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Friends Seminary 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. Friends Seminary 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4801.

Very truly yours,

Alexander T. Walker of
MULLEN COUGHLIN LLC

ATW/msf

EXHIBIT A

November 11, 2020

Dear Friend,

We are writing to inform you of an incident involving one of our third-party vendors, Blackbaud, Inc. ("Blackbaud") that may affect the privacy of some of your personal information. We want to be clear that although this incident was disclosed to Friends Seminary by Blackbaud in July of this year, on September 29, 2020, and in contradiction of multiple written statements previously made by Blackbaud, Friends Seminary learned that personal information was potentially impacted by the incident. This notice provides information about the Blackbaud incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so. In order to best comply with applicable requirements under the law, we anticipate sending you a similar notice to this one via U.S. mail in the coming days.

What Happened? On Thursday, July 16, 2020, Friends Seminary, along with countless other businesses, received notification from one of its third-party vendors, Blackbaud, of a cyber incident that occurred in Blackbaud's systems. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to organizations, including Friends Seminary. Upon receiving notice of the cyber incident, we immediately commenced an investigation to better understand the nature and scope of the incident and any impact on Friends Seminary data. Blackbaud originally 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 the nature and scope of the incident. Following its investigation, Blackbaud notified its customer organizations 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.

Upon learning of this event, Friends Seminary immediately commenced an investigation to determine what, if any, sensitive data relating to us was potentially affected. Blackbaud initially reported to us that this incident did not impact information such as Social Security numbers or bank account information. However, on September 29, 2020, Friends Seminary received further information from Blackbaud that expanded the types of data impacted. On or about October 16, 2020, Friends Seminary confirmed the types of personal information potentially affected and that it applies to individuals including some of our current employees. In an abundance of caution, we continue to investigate to confirm Blackbaud's investigation and better understand what occurred.

What Information Is Involved? Initially Blackbaud advised us that, based on its investigation, the accessed files did not contain any unencrypted credit card information, bank account information, or Social Security numbers, and the cybercriminal did not access any encryption key. However, upon further investigation by Blackbaud, it was determined that Social Security numbers, bank account information and other payroll information were, in fact, present in a payroll table from a legacy version of the financial services tool which remained after we converted to a new tool. Please note that, to date, we have not received specific confirmation from Blackbaud that your specific information was accessed or acquired by the unknown actor. Rather we understand Blackbaud cannot rule out that your personal information may have been subject to unauthorized access or acquisition. Nonetheless, Friends Seminary worked with Blackbaud to provide access for employees to 2 years of identity and credit monitoring services through Experian, at no costs to our employees.

The confidentiality, privacy, and security of information in our care are among our highest priorities, as you know, and we take this incident very seriously. As part of our ongoing commitment to the security of information in our care, we are working to review our existing policies and procedures regarding our third-party vendors, and are working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. We will also be notifying certain regulators, as required.

We encourage you to review the enclosed *Steps You Can Take to Help Protect Your Information*. There you will find general information on what you can do to help protect your personal information.

We understand that you may have questions about the Blackbaud incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 855-914-4670 between the hours of 9:00 a.m. and 9:00 p.m. EST.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

Sisi Komal
Chief Financial and Operating Officer

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

We are providing you with access to **Single Bureau Credit Monitoring** services through Experian at no charge. Services are for 24 months from the date of enrollment. When changes occur to your Experian credit file, notification is sent to you the same day the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud you will also have access remediation support from a CyberScout Fraud Investigator.

To enroll in Credit Monitoring services at no charge, please navigate to:
[redacted]

If prompted, please provide the following unique code to gain access to services: [redacted]

Once registered, you can access Monitoring Services by selecting the "Use Now" link to fully authenticate your identity and activate your services. **Please ensure you take this step to receive your alerts.**

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

Monitor Accounts

In general, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. 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 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	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

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

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 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	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

Additional Information

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 also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.

***New York Residents*:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

EXHIBIT B

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>> <<Date>>
<<Country>>

Dear <<Name 1>>:

We are writing in follow up to the email sent on November 12, 2020 in order to inform you of an incident involving one of our third-party vendors, Blackbaud, Inc. ("Blackbaud") that may affect the privacy of some of your personal information. We want to be clear that although this incident was disclosed to Friends Seminary by Blackbaud in July of this year, on September 29, 2020, and in contradiction of multiple written statements previously made by Blackbaud, Friends Seminary learned that personal information was potentially impacted by the incident. This notice provides information about the Blackbaud incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it necessary to do so. In order to best comply with applicable requirements under the law, we anticipate sending you a similar notice to this one via U.S. mail in the coming days.

What Happened? On Thursday, July 16, 2020, Friends Seminary, along with countless other businesses, received notification from one of its third-party vendors, Blackbaud, of a cyber incident that occurred in Blackbaud's systems. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to organizations, including Friends Seminary. Upon receiving notice of the cyber incident, we immediately commenced an investigation to better understand the nature and scope of the incident and any impact on Friends Seminary data. Blackbaud originally 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 the nature and scope of the incident. Following its investigation, Blackbaud notified its customer organizations 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.

Upon learning of this event, Friends Seminary immediately commenced an investigation to determine what, if any, sensitive data relating to us was potentially affected. Blackbaud initially reported to us that this incident did not impact information such as Social Security numbers or bank account information. However, on September 29, 2020, Friends Seminary received further information from Blackbaud that expanded the types of data impacted. On or about October 16, 2020, Friends Seminary confirmed the types of personal information potentially affected and that it

applies to individuals including some of our current employees. In an abundance of caution, we continue to investigate to confirm Blackbaud's investigation and better understand what occurred.

What Information Is Involved? Initially Blackbaud advised us that, based on its investigation, the accessed files did not contain any unencrypted credit card information, bank account information, or Social Security numbers, and the cybercriminal did not access any encryption key. However, upon further investigation by Blackbaud, it was determined that Social Security numbers, bank account information and other payroll information were, in fact, present in a payroll table from a legacy version of the financial services tool which remained after we converted to a new tool. Please note that, to date, we have not received specific confirmation from Blackbaud that your specific information was accessed or acquired by the unknown actor. Rather we understand Blackbaud cannot rule out that your personal information may have been subject to unauthorized access or acquisition. Our investigation determined that the following information related to you may have been present in the legacy payroll table at the time of the incident: <<Data Elements>>, and name. Nonetheless, Friends Seminary worked with Blackbaud to provide access for employees to 2 years of identity and credit monitoring services through Experian, at no cost to our employees.

The confidentiality, privacy, and security of information in our care are among our highest priorities, as you know, and we take this incident very seriously. As part of our ongoing commitment to the security of information in our care, we are working to review our existing policies and procedures regarding our third-party vendors, and are working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. We will also be notifying certain regulators, as required.

We encourage you to review the enclosed *Steps You Can Take to Help Protect Your Information*. There you will find general information on what you can do to help protect your personal information.

We understand that you may have questions about the Blackbaud incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 855-914-4670 Monday through Friday, between the hours of 9:00 a.m. and 9:00 p.m. EST.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

Sisi Kamal
CFO/COO

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

We are providing you with access to **Single Bureau Credit Monitoring** services through Experian at no charge. Services are for 24 months from the date of enrollment. When changes occur to your Experian credit file, notification is sent to you the same day the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud you will also have access remediation support from a CyberScout Fraud Investigator.

To enroll in Credit Monitoring services at no charge, please navigate to:
[redacted]

If prompted, please provide the following unique code to gain access to services: [redacted]

Once registered, you can access Monitoring Services by selecting the "Use Now" link to fully authenticate your identity and activate your services. **Please ensure you take this step to receive your alerts.**

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

Monitor Accounts

In general, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. 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 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	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

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;

6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

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
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

Additional Information

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 also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.

***New York Residents*:** the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.