



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Amanda Harvey
Office: (267) 930-1697
Fax: (267) 930-4771
Email: aharvey@mullen.law

4843 Colleyville Blvd, Suite 251-388
Colleyville, TX 76034

September 4, 2020

VIA FIRST-CLASS MAIL

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

2020 SEP -8 PM 1:06
STATE OF NH
DEPT OF JUSTI

Re: Notice of Data Event

Dear Sir or Madam:

We represent Vermont Student Assistance Corporation (“VSAC”) located at 10 E Allen Street, Winooski, Vermont 05404-2291, and are writing to notify your office of an incident that may affect the security of some personal information relating to one thousand seventeen (1,017) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, VSAC 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, VSAC received notification from one of its third-party vendors, Blackbaud, Inc. (“Blackbaud”), of a cyber incident. Blackbaud is a cloud computing provider that offers financial services tools to organizations, including VSAC. Upon receiving notice of the cyber incident, VSAC immediately commenced an investigation to better understand the nature and scope of the incident and any impact on VSAC data.

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 consultants to investigate. Following its investigation, Blackbaud notified its customers, including VSAC, 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 the Blackbaud incident, VSAC immediately commenced an investigation to determine what, if any, sensitive VSAC data was potentially involved. This investigation included working diligently to gather further information from Blackbaud to understand the

scope of the incident. On or about July 31, 2020, VSAC's investigation determined that the information potentially affected may have contained personal information.

The information that could have been subject to unauthorized access includes names and Social Security numbers.

Notice to New Hampshire Residents

On or about September 4, 2020 VSAC began providing written notice of this incident to all affected individuals, which includes one thousand seventeen (1,017) New Hampshire 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

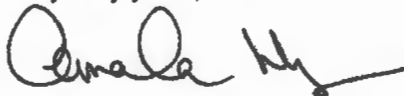
Upon learning of this incident, VSAC moved quickly to assess the data potentially at risk and to notify potentially impacted individuals. VSAC is reviewing its existing policies and procedures regarding its third-party vendors and working with Blackbaud to evaluate additional measures and safeguards to protect against this type of incident in the future. VSAC offered complimentary access to 12 months of credit monitoring services, including identity theft restoration services, through Experian to individuals whose personal information was potentially affected by this incident, at no cost to these individuals. VSAC also established a dedicated call center for potentially affected individuals to call with questions or concerns regarding this incident.

Additionally, VSAC is providing impacted individuals with guidance on how to better protect against identity theft and fraud. VSAC is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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) 930-1697.

Very truly yours,

A handwritten signature in black ink, appearing to read "Amanda Harvey", with a long horizontal flourish extending to the right.

Amanda Harvey of
MULLEN COUGHLIN LLC

EXHIBIT A



Return Mail Processing
 PO Box 589
 Claysburg, PA 16625-0589

September 4, 2020

F7642-L01-0000001 P001 T00001 *****MIXED AADC 159



SAMPLE A SAMPLE - L01 GENERAL
 APT 123
 123 ANY ST
 ANYTOWN, US 12345-6789



Dear Sample A Sample:

Vermont Student Assistance Corporation (“VSAC”) is writing to inform you of a recent incident that may affect the security of some of your information. On July 16, 2020, VSAC received notice that one of its third-party vendors, Blackbaud, Inc. (“Blackbaud”), suffered a cyber incident. Blackbaud is a cloud computing provider that offers customer relationship management and financial services tools to many non-profit organizations, including VSAC. While we are unaware of any actual or attempted misuse of your information, we are providing you with information about the incident, our response, and steps you may take to better protect yourself, should you feel it necessary to do so.

What Happened? In May 2020, Blackbaud experienced a ransomware incident that impacted certain systems within the Blackbaud environment. As a result of this incident, certain Blackbaud systems were encrypted and a Blackbaud database backup file including VSAC data was removed from the Blackbaud environment by an unauthorized actor. While Blackbaud’s investigation was able to determine that the backup file was removed between February 7, 2020 and May 20, 2020, their investigation was unable to confirm exactly when this occurred. As a result, the unauthorized actor may have had access to certain information contained within the backup database. Upon learning of this incident, VSAC immediately began an investigation to determine the full nature and scope of the event and what, if any, VSAC data may have been impacted. On or about August 7, 2020, VSAC’s investigation determined that the backup database may have contained personal information.

What Information Was Involved? While Blackbaud reports that information was accessed, Blackbaud was unable to confirm what, if any, specific sensitive information was actually accessed or acquired by the unauthorized actor. Blackbaud has also represented to us that they “have 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.” Regardless, out of an abundance of caution, VSAC is notifying you of this incident because you are or were a customer or client of VSAC, and information related to you was potentially present in the database at the time of this incident. Our investigation determined that the information related to you included your name and Social Security number. To date, VSAC has not received any reports of actual or attempted misuse of your information.



What Are We Doing? The confidentiality, privacy, and security of information in our care is one of our highest priorities and we take this incident very seriously. When we were notified of this incident, we immediately commenced an investigation to determine what VSAC data may have been at risk. 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 are also notifying state and federal regulators, as required.

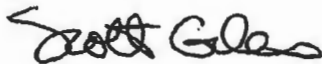
As an added precaution, we are also offering you complimentary access to 12 months of credit monitoring and identity theft restoration services through Experian. We encourage you to enroll in these services, as we are not able to act on your behalf to enroll you. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Information* for additional information on these services.

What Can You Do? We encourage you to review the enclosed *Steps You Can Take To Help Protect Your Information* for additional steps you may take and information on what you can do to better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so. You may also enroll to receive the free credit and identity monitoring services we are offering.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at (844) 866-3863 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number DB22323. You may also write to VSAC at 10 E Allen Street, attn: Customer Service, Winooski, Vermont 05404.

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

Sincerely,



Scott Giles
President and CEO
Vermont Student Assistance Corporation

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit and Identity Monitoring

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 12 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by November 30th, 2020** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (844) 866-3863 by November 30th, 2020. Be prepared to provide engagement number DB22323 as proof of eligibility for the Identity Restoration services by Experian.

000001



F7642-L01

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.¹
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Monitor Accounts

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

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

[www.experian.com/freeze/
center.html](http://www.experian.com/freeze/center.html)

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

[www.transunion.com/
credit-freeze](http://www.transunion.com/credit-freeze)

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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); 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. This notice has not been delayed by law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

0000001



F7642-L01

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For 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/>.

For Rhode Island residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 179 Rhode Island residents impacted by this incident.

