MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

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

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

February 1, 2021

VIA E-MAIL
Office of the Attorney General
1135 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-mail: securitybreach@atg.wa.gov

Re: Supplemental Notice of Data Event

Dear Sir or Madam:

We continue to represent Convoy of Hope ("COH") located at 330 S. Patterson Ave., Springfield, Missouri 65802 and write to supplement our January 8, 2021, notice to your Office regarding an incident that may affect the security of some personal information relating Washington residents. This notice maybe supplemented if any new significant facts are learned subsequent to its submission. By providing this notice, COH does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

In July 2020, COH received notice from Blackbaud of a cybersecurity event that occurred on their systems that was discovered in May of 2020. The notice advised that a subset of data was taken from the Blackbaud systems, including data potentially related to COH. COH was not using Blackbaud for these services at the time of this incident; however, COH learned that Blackbaud was maintaining certain data related to COH from a previous period where Blackbaud was a COH vendor. While Blackbaud has not confirmed what data specifically relating to COH was involved in the event, it advised that backup copies of data were accessed or acquired during the event. However, COH did not have access to the data identified by Blackbaud because COH was no longer a customer, and as such, COH was required to work with and rely upon Blackbaud to provide information necessary to determine the potential impact on COH data.

Following extensive communications with Blackbaud, on October 9, 2020, Blackbaud provided additional information to COH related to the potentially impacted information. However, because COH is no longer a customer of Blackbaud, the information was provided in a format that was not

readable to COH. As such, COH began working with third party computer specialists to obtain this information in a readable format and reviewing the data set to determine what records were present. On December 9, 2020, COH obtained the necessary information to allow COH to determine what data was potentially impacted by the Blackbaud event. Pursuant to a review of the information provided by Blackbaud, COH determined that personal information relating to certain individuals, including information for one-thousand seventeen (1,017) Washington residents, was present on Blackbaud's system at the time of the event. The type of information for potentially impacted Washington residents includes name and date of birth.

Notice to Washington Residents

As previously reported, on January 8, 2021, COH began providing written notice of this incident to potentially impacted individuals, including twenty (20) Washington residents. Following the initial notice, COH continued to review the data and work to provide notice to all potentially affected Washington residents. On January 21, 2021, COH completed this review and confirmed that the data included an additional nine hundred ninety-seven (997) Washington residents. On February 1, 2021, COH began providing written notice of this incident to the additional nine hundred ninety-seven (997) potentially impacted Washington 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, COH moved quickly to investigate and respond to the incident and to notify potentially affected individuals. This included coordination with Blackbaud to confirm what information may have been affected by Blackbaud's incident. COH is reviewing existing policies and procedures regarding third-party vendors and is working with Blackbaud to ensure COH data is appropriately removed from the system.

COH is also providing individuals with guidance on how to better protect against identity theft and fraud, including 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) 930-4773.

Very truly yours,

M. Alexandra Belton of
MULLEN COUGHLIN LLC

MABB/jc1
Enclosure

Exhibit A

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>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

Convoy of Hope ("COH") writes to notify you of the Blackbaud, Inc. ("Blackbaud") data security incident because we believe your name and date of birth may have been affected. Blackbaud provides data services for thousands of nonprofits worldwide. We were not using Blackbaud for these services at the time of this incident; however, we learned that Blackbaud was maintaining certain data related to COH from a previous period when they were our vendor. To date, Blackbaud has not reported that your information has been misused as a result of this incident. Nevertheless, we are notifying you so that you are aware of the incidentand may take steps to better protect your information, should you feel it appropriate to do so.

In July 2020, we received notice from Blackbaud of a cybersecurity event that occurred on their systems that was discovered in May of 2020. The notice advised that a subset of data was taken from the Blackbaud systems, including data potentially related to COH. While Blackbaud has not confirmed what data specifically relating to COH was involved in the event, it advised that backup copies of data were accessed or acquired during the event. However, we did not have access to the data identified by Blackbaud because we were no longer using Blackbaud's services. As such, we worked with and relied upon Blackbaud to provide information necessary to determine the potential impact on our data.

Following extensive communications with Blackbaud, on October 9, 2020, Blackbaud provided additional information to COH related to the potentially impacted information. However, because we are no longer a client of Blackbaud, the information was provided in a format that was not readable to COH. As such, we began working with third-party computer specialists to obtain this information in a readable format and review the information to confirm what data was present. On December 9, 2020, we obtained the necessary information to allow us to determine what data was potentially impacted by the Blackbaud event. Pursuant to a review of this information provided by Blackbaud, we determined that personal information relating to certain individuals, including you, was present on Blackbaud's system at the time of the event. The type of information included your name and date of birth.

The security of information in our care is very important to us. As part of our ongoing commitment to the security of information,we are reviewing our existing policies and procedures regarding our third-party vendors and are working with Blackbaud to ensure COH data is appropriately removed from the system.

We have also enclosed the attached "Steps You Can Take to Protect Your Information" for further details on resources available to protect your personal information.

We understand you may have questions about this incident that are not addressed in this letter. If you have questions, please contact us at (417) 851-4466. You may also contact COH by mail at 330 S. Patterson Avenue, Springfield, MO 65802. Protecting your information is important to us, and we remain committed to safeguarding the information in our care.

Sincerely,

Dr. Kregg Hood

Senior Vice President & Chief Operations Officer

Steps You Can Take to Protect Your Information

Monitor Your Accounts

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 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

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.

For Maryland residents, the Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; or www.oag.state.md.us.

MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

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

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

January 8, 2021

VIA E-MAIL

Office of the Attorney General
1135 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100
E-mail: securitybreach@atg.wa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent Convoy of Hope ("COH") located at 330 S. Patterson Ave, Springfield, MO 65802 and write to notify your Office of an incident that may affect the security of some personal information relating to certain Washington residents. This notice may be supplemented if any new significant facts are learned subsequent to its submission. By providing this notice, COH does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

In July 2020, COH received notice from Blackbaud of a cybersecurity event that occurred on their systems that was discovered in May of 2020. The notice advised that a subset of data was taken from the Blackbaud systems, including data potentially related to COH. COH was not using Blackbaud for these services at the time of this incident; however, COH learned that Blackbaud was maintaining certain data related to COH from a previous period where Blackbaud was a COH vendor. While Blackbaud has not confirmed what data specifically relating to COH was involved in the event, it advised that backup copies of data were accessed or acquired during the event. However, COH did not have access to the data identified by Blackbaud because COH was no longer a customer, and as such, COH was required to work with and rely upon Blackbaud to provide information necessary to determine the potential impact on COH data.

Following extensive communications with Blackbaud, on October 9, 2020, Blackbaud provided additional information to COH related to the potentially impacted information. However, because COH is no longer a customer of Blackbaud, the information was provided in a format that was not readable to COH. As such, COH began working with third party computer specialists to obtain this information in a readable format and reviewing the data set to determine what records were present. On December 9, 2020, COH obtained the necessary information to allow COH to determine what data was potentially impacted by the Blackbaud

event. While the review of the information provided by Blackbaud remains ongoing at this time, COH determined that personal information relating to certain individuals, including Washington residents, was present on Blackbaud's system at the time of the event. The type of information for potentially impacted Washington residents includes name and date of birth.

Notice to Washington Residents

On January 8, 2021, COH began providing written notice of this incident to potentially impacted individuals, including approximately twenty (20) Washington residents. COH's effort to review the data and confirm the number of affected Washington residents, as well as the effort to provide notification, are ongoing. This notice will be supplemented with additional information as these efforts continue. 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, COH moved quickly to investigate and respond to the incident and to notify potentially affected individuals. This included coordination with Blackbaud to confirm what information may have been affected by Blackbaud's incident. COH is reviewing existing policies and procedures regarding third-party vendors and is working with Blackbaud to ensure COH data is appropriately removed from the system.

COH is also providing individuals with guidance on how to better protect against identity theft and fraud, including 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) 930-4773.

Very truly yours,

M. Alexandra Belton of
MULLEN COUGHLIN LLC

MABB/jc1
Enclosure

[First Name] [Last Name]
[Address]
[City, State, Zip]

[DATE]

Dear [Name]

Convoy of Hope ("COH") writes to notify you of the Blackbaud, Inc. ("Blackbaud") data security incident because we believe your name and **[DATA]** may have been affected. Blackbaud provides data services for thousands of nonprofits worldwide. We were not using Blackbaud for these services at the time of this incident; however, we learned that Blackbaud was maintaining certain data related to COH from a previous period when they were our vendor. To date, Blackbaud has not reported that your information has been misused as a result of this incident. Nevertheless, we are notifying you so that you are aware of the incident and may take steps to better protect your information, should you feel it appropriate to do so.

In July 2020, we received notice from Blackbaud of a cybersecurity event that occurred on their systems that was discovered in May of 2020. The notice advised that a subset of data was taken from the Blackbaud systems, including data potentially related to COH. While Blackbaud has not confirmed what data specifically relating to COH was not involved in the event, it advised that backup copies of data were accessed or acquired during the event. However, we did not have access to the data identified by Blackbaud because we were no longer using Blackbaud's services. As such, we worked with and relied upon Blackbaud to provide information necessary to determine the potential impact on our data.

Following extensive communications with Blackbaud, on October 9, 2020, Blackbaud provided additional information to COH related to the potentially impacted information. However, because we are no longer a client of Blackbaud, the information was provided in a format that was not readable to COH. As such, we began working with third-party computer specialists to obtain this information in a readable format and review the information to confirm what data was present. On December 9, 2020, we obtained the necessary information to allow us to determine what data was potentially impacted by the Blackbaud event. Pursuant to a review of this information provided by Blackbaud, we determined that personal information relating to certain individuals, including you, was present on Blackbaud's system at the time of the event. The type of information included your name and **[DATA]**.

The security of information in our care is very important to us. As part of our ongoing commitment to the security of information, we are reviewing our existing policies and procedures regarding our third-party vendors and are working with Blackbaud to ensure COH data is appropriately removed from the system.

We have also enclosed the attached "Steps You Can Take to Protect Your Information" for further details on resources available to protect your personal information.

We understand you may have questions about this incident that are not addressed in this letter. If you have questions, please contact us at (417) 851-4466. You may also contact COH by mail at 330 S. Patterson Avenue, Springfield, MO 65802. Protecting your information is important to us, and we remain committed to safeguarding the information in our care.

Sincerely,

Dr. Kregg Hood
Senior Vice President & Chief Operations Officer

Enclosures

Steps You Can Take to Protect Your Information

Monitor Your Accounts

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 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

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.

For Maryland residents, the Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; or www.oag.state.md.us.