



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED

DEC 20 2019

CONSUMER PROTECTION

Ryan C. Loughlin
Office: 267-930-4786
Fax: 267-930-4771
Email: rloughlin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

December 16, 2019

VIA U.S. MAIL

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

Re: Supplemental Notice of Data Security Incident

Dear Sir or Madam:

We continue to represent Arthur J. Gallagher & Co. ("Gallagher") located at 2850 Golf Road, Rolling Meadows, Illinois 60008. We write to supplement our November 26, 2019 and December 4, 2019 notices to your office. 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 supplemental notice, Gallagher 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.

Based on the ongoing investigation and response, Gallagher is mailing notice to additional individuals whose personal information may have been accessible including ninety-eight (98) additional New Hampshire residents on December 16, 2019 in substantially the same form as the letter attached hereto as *Exhibit CC*.

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4786.

Very truly yours,

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL:gcl
Enclosure

EXHIBIT CC



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>>:

Gallagher Bassett Services, Inc. (“Gallagher”), a third-party administrator handling claims on behalf of your employer and your employer’s insurer, [REDACTED], is writing to notify you of an incident that may affect the security of some of your personal information. Gallagher received your information as part of the normal course of claims services it provides. While we are unaware of any actual or attempted misuse of your information, we want to provide you with information about the incident, our response, and steps you may take to better protect against possible misuse of your personal information, should you feel it appropriate to do so.

What Happened? Without Gallagher’s awareness or permission, an individual at an outside law firm assisting with legal proceedings transferred data provided on an encrypted drive to an unencrypted hard drive and subsequently misplaced the drive while traveling. The law firm notified Gallagher about the incident on or around March 15, 2019. Upon learning of the incident, Gallagher immediately launched an investigation, including working with several third-party investigators and experts, to try to locate the missing hard drive and also to confirm the nature and scope of the data involved. During that time, Gallagher was informed that the outside law firm had not yet refined and identified the relevant data for the legal matter, and the individual lawyer transferred all the data provided to it from Gallagher onto the unencrypted hard drive. In the middle of October 2019, Gallagher determined that your personal information was also contained on the hard drive.

What Information was Involved? Through the manual and programmatic review of the drive contents, we determined that the information present on the drive included your <<Breached Elements>>. **To date, Gallagher has not received any reports of actual or attempted misuse of your information and has no evidence that the information on the drive has been accessed.**

What We Are Doing. The confidentiality, privacy, and security of information in our care is one of Gallagher’s highest priorities and we take this incident very seriously. Since we learned of this incident, we have been working diligently to determine what happened and what personal data was involved. We also engaged in significant discussion with the law firm involved that moved the data from the encrypted drive it was provided. As part of our ongoing commitment to the security of personal information in our care, we are working to retrain third-party business partners on our policies and procedures for how they handle and safeguard the data we provide them. We also will be notifying regulatory authorities, as required by law.

As an added precaution, we are also offering you complimentary access to one year of credit monitoring and identity theft restoration services through TransUnion. 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 Protect Your Information* for additional information on these services.

What You Can Do. While we have no evidence that the information on the drive has been accessed, you can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Protect Your Information*. There you will also find more information on the credit monitoring services we are offering and how to enroll.

For More Information. We understand you may have questions that are not answered in this letter. If you have questions, please contact 833-935-0815 Monday through Friday from 9:00 a.m. to 9:00 p.m. EST.

Sincerely,

A handwritten signature in black ink, appearing to read "Mark Lechowicz". The signature is fluid and cursive, with a long, sweeping tail on the final letter.

Mark Lechowicz
Chief Compliance Officer
Gallagher Bassett Services, Inc.

Steps You Can Take to Protect Your Information

Complimentary One-Year *myTrueIdentity* Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,[®] one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *myTrueIdentity* website at **www.MyTrueIdentity.com** and, in the space referenced as “Enter Activation Code,” enter the 12-letter Activation Code <<**Insert Unique 12-letter Activation Code**>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode <<**Insert static 6-digit Telephone Pass Code**>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<**Enrollment Deadline**>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

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

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

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-alerts

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.

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 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 violators. 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_cfbp_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 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/>.



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>>:

Gallagher Bassett Services, Inc. (“Gallagher”) is writing to notify you of an incident that may affect the security of some of your personal information. Gallagher received your information as part of the normal course of claims services it provides. While we are unaware of any actual or attempted misuse of your information, we want to provide you with information about the incident, our response, and steps you may take to better protect against possible misuse of your personal information, should you feel it appropriate to do so.

What Happened? Without Gallagher’s awareness or permission, an individual at an outside law firm assisting with legal proceedings transferred data provided on an encrypted drive to an unencrypted hard drive and subsequently misplaced the drive while traveling. The law firm notified Gallagher about the incident on or around March 15, 2019. Upon learning of the incident, Gallagher immediately launched an investigation, including working with several third-party investigators and experts, to try to locate the missing hard drive and also to confirm the nature and scope of the data involved. During that time, Gallagher was informed that the outside law firm had not yet refined the data for the legal matter, and the individual lawyer transferred all the data provided to it from Gallagher onto the unencrypted hard drive. In the middle of October 2019, Gallagher determined that your personal information was also contained on the hard drive.

What Information was Involved? Through the manual and programmatic review of the drive contents, we determined that the information present on the drive included your <<Breached Elements>>. **To date, Gallagher has not received any reports of actual or attempted misuse of your information and has no evidence that the information on the drive has been accessed.**

What We Are Doing. The confidentiality, privacy, and security of information in our care is one of Gallagher’s highest priorities and we take this incident very seriously. Since we learned of this incident, we have been working diligently to determine what happened and what personal data was involved. We also engaged in significant discussion with the law firm involved that moved the data from the encrypted drive it was provided. As part of our ongoing commitment to the security of personal information in our care, we are working to retrain third-party business partners on our policies and procedures for how they handle and safeguard the data we provide them. We also will be notifying regulatory authorities, as required by law.

As an added precaution, we are also offering you complimentary access to two years of credit monitoring and identity theft restoration services through TransUnion. 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 Protect Your Information* for additional information on these services.

What You Can Do. While we have no evidence that the information on the drive has been accessed, you can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Protect Your Information*. There you will also find more information on the credit monitoring services we are offering and how to enroll.

For More Information. We understand you may have questions that are not answered in this letter. If you have questions, please contact 833-935-0815 Monday through Friday from 9:00 a.m. to 9:00 p.m. EST.

Sincerely,

A handwritten signature in black ink, appearing to read 'Mark Lechowicz', written in a cursive style.

Mark Lechowicz
Chief Compliance Officer
Gallagher Bassett Services, Inc.

Steps You Can Take to Protect Your Information

Complimentary Two-Year *myTrueIdentity* Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for two years provided by TransUnion Interactive, a subsidiary of TransUnion,[®] one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as “Enter Activation Code,” enter the 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode <<Insert static 6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

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)

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-alerts

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 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 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.

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 violators. 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 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; www.ag.ny.gov.

For Iowa residents, the Attorney General can be contacted at 1305 E. Walnut St, Des Moines, IA 50319, 1-515-281-5926 or 1-888-777-4590; www.iowaattorneygeneral.gov.

For Oregon residents, the Attorney General can be contacted at 1162 Court Street NE, Salem, OR 97301-4096 1-877-877-9392; www.doj.state.or.us.