MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Paul T. McGurkin, Jr.
Office: 267-930-4788
Fax: 267-930-4771
Email: pmcgurkin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

December 26, 2018

VIA REGULAR MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General MacDonald:

Our office represents 4A's Benefits located at 11020 David Taylor Drive, Suite 305, Charlotte, NC 28262-1103. 4A's Benefits provides administration and record keeping services for retirement plans offered by its member agencies. We write on behalf of the plan sponsors listed on **Exhibit A** to notify you of an event that may affect the security of personal information relating to one (1) New Hampshire resident who are participants in the retirement plans. This notice may be supplemented where additional 4A's Benefits plan sponsors request notice be provided on their behalf. By providing this notice, 4A's Benefits and the plan sponsors do 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.

Background

On July 19, 2018, 4A's Benefits determined that a 4A's Benefits employee's email account was subject to unauthorized access between the dates of December 6 and December 12, 2017. The available forensic evidence was unable to confirm what, if any, emails were subject to unauthorized access during that time. Therefore, in an abundance of caution, a vendor was retained to undertake an extensive and time-consuming review of the contents of the impacted email account to see whether it housed any protected information. On October 1, 2018, 4A's Benefits determined the affected email account contained information related to one (1) New Hampshire resident. However, this file did not include agency affiliation or addresses for most of the individuals. Since receiving the list, significant work was performed at 4A's Benefits to match affected individuals back to the appropriate plan sponsor/member agency. On November 29, 2018, 4A's Benefits mailed notice of the incident to the impacted plan sponsors who are in existence[1] and received permission to notify affected individuals on their behalf.

[1] A small number of plan sponsors are no longer in existence. Participants affiliated with these plan sponsors were notified directly by 4A's.

The forensic investigation was unable to confirm whether the personal information housed within the email account was subject to unauthorized access. The investigation was only able to confirm that the personal information was found within an email account subject to unauthorized access. The information found in the email account related to the one (1) New Hampshire resident includes name, address, date of birth and Social Security number.

Notice to New Hampshire Resident

4A's Benefits will begin mailing written notice of this incident to the affected New Hampshire resident on December 26, 2018, in substantially the same form as the letter attached hereto as ***Exhibit B***.

Other Steps Taken and To Be Taken

4A's Benefits is offering individuals impacted by this event with access to one (1) year of complimentary credit monitoring and identity restoration services. Additionally, 4A's Benefits is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including 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. 4A's Benefits is also taking steps to mitigate the risk that an event like this will happen again by reviewing its policies and procedures and has implemented additional safeguards which include:

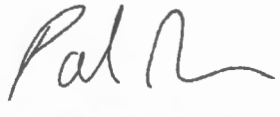
- Passing penetration testing on all internal systems by an outside security firm
- The deployment of multi-factor authentication to all 4A's Benefits email accounts
- The addition of software which blocks the transmission of certain sensitive information via email either to or from 4A's Benefits emails accounts
- Hardened the existing participant password rules for Retirement Plan account access
- In process of deploying multi-factor authentication for the Retirement Fund Website

In addition to providing this notice to your office, 4A's Benefits is providing notice to other state regulators and the consumer reporting agencies, as required.

Contact Information

Should you have any questions regarding this notification of other aspects of this event, please contact us at 267-930-4788.

Very truly yours,



Paul T. McGurkin of
MULLEN COUGHLIN LLC

PTM:ncl
Enclosure

EXHIBIT A

Plan Sponsors

Grey Healthcare

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>>
<<Country>>

<<Date>>

RE: Notice of Data Breach, <<Company>> <<Client_def1>>

Dear <<Name 1>>:

4A's Benefits is writing to notify you of a recent security incident that may impact your personal information. 4A's Benefits provides administration and record keeping services for retirement plans offered by its member agencies. Although we are unaware of any actual access or attempted misuse of your information, we are providing you with information regarding the incident, steps we have taken since discovering the incident, and what you can do to protect against identity theft should you feel it is appropriate to do so.

What Happened? 4A's Benefits determined that a 4A's Benefits employee's email account was subject to unauthorized access between the dates of December 6 and December 12, 2017. The available forensic evidence was unable to confirm what, if any, emails were subject to unauthorized access during that time. Therefore, in an abundance of caution, a vendor was retained to undertake an extensive and time-consuming review of the contents of the impacted email account to see whether it housed any protected information. On October 1, 2018, 4A's Benefits was provided with a list of potentially impacted individuals whose protected information was found within the email account. On November 29, 2018, 4A's Benefits mailed notice to your employer/former employer and received permission to provide you with this notice.

What Information Was Involved? The information related to you stored within the impacted email included your name, address, social security number, and possibly your date of birth. The forensic investigation was unable to confirm if your personal information was accessed by an unauthorized actor. We were only able to confirm that your information was found within the email account subject to unauthorized access.

What We Are Doing. 4A's Benefits has no indication that any fraud has resulted from this incident. We have security measures in place to protect the data on our systems and we have placed additional safeguards and conducted internal employee training in response to this incident. We are offering you free credit monitoring services and identity restoration services through TransUnion.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online, three-bureau 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, three-bureau 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 six-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 three-bureau credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion,® Experian,® and Equifax,® 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.)

What You Can Do. You can enroll in the services being offered to receive free credit monitoring and identity restoration services. You can also review the enclosed "Steps You Can Take to Prevent Identity Theft and Fraud." In addition, we advise you to report suspected incidents of identity theft to local law enforcement or State Attorney General.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. We have established a confidential, toll-free hotline to assist you with questions regarding this incident, the free services we are making available, and steps you can take to protect yourself against identity theft and fraud. The hotline is available at 877-854-8631, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time.

We apologize for any inconvenience this may cause you.

Sincerely,
4A's Benefits

Steps You Can Take to Protect Against Identity Theft and Fraud

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**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-800-909-8872	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 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more 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. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, 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 Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are two Rhode Island residents impacted by this incident.