WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

February 26, 2021

Michael E. Kar, Esq.
212.915.5535 (direct)
Michael.Kar@WilsonElser.com

Via electronic-mail: *DOJ-CPB@doj.nh.gov; AttorneyGeneral@doj.nh.gov*

Attorney General Gordon McDonald
Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re:	**Our Client**	**:**	**AllyAlign Health, Inc.**
	Matter	**:**	**November 14, 2020 Data Security Incident**
	Wilson Elser File #	**:**	**16516.01237**

Dear Attorney General McDonald:

We represent AllyAlign Health, Inc. ("AAH"), with a principle place of business in Glen Allen, Virginia with respect to a potential data security incident described in more detail below. AAH takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the security breach, the number of New Hampshire residents being notified, what information has been compromised, and the steps that AAH is taking to secure the integrity of its systems. We have also enclosed hereto a sample of the notification made to the potentially impact individuals, which includes an offer of free credit monitoring.

1. Nature of the Security Incident

AAH is a Medicare Advantage special needs plan administrator headquartered in Richmond, Virginia. On November 14, 2020, AAH detected that it was the target of a cybersecurity attack. An unauthorized third party attempted to infiltrate the AAH's computer network, lock-out AAH, and then demand a ransom payment.

Through counsel, AAH immediately commenced a comprehensive third-party forensic investigation. This forensic investigation concluded on February 2, 2021.

AAH has found no evidence that specific individuals' information has been specifically accessed or acquired for misuse. However, due to the compromise of AAH's network, AAH has notified all

potentially affected individuals of this incident. Individuals were notified that the following data points could have been exposed to the cybercriminal:

i. For AAH members, potentially exposed information included full name, address, date of birth, social security number, Medicare Health Insurance Claim Number (HICN), Medicare Beneficiary Identifier (MBI), Medicaid recipient identification number (if applicable), medical claims history, health insurance policy number, and other medical information.

ii. For AAH employees and associated medical providers, potentially exposed information included full name, address, date of birth, and social security number.

As of this writing, AAH has not received any reports of related identity theft since the date of the incident (November 14, 2020 to present).

2. Steps Taken

Immediately upon learning of this incident, AAH contacted a reputable third-party forensic team to assist with its investigation. Since then, AAH has been working with cybersecurity experts to review all policies and procedures relating to the security of AAH's systems, as well as its information life cycle management.

Although AAH is not aware of any evidence of misuse of personal information, AAH extended to all potentially impacted individuals an offer for free credit monitoring and identity theft protection through IDX. This service will include at least 12 months of credit monitoring, along with a fully managed identity theft recovery service, should the need arise.

3. Contact Information

AAH remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Michael.Kar@WilsonElser.com or 212.915.5535.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Michael E. Kar, Esq.

Copy: Robert Walker, Esq. (Wilson Elser LLP)
Tawana Johnson, Esq.

Enclosure: *Sample Notification Letter*

AllyAlign Health
C/O IDX
PO Box 4129
Everett WA 98204

ENDORSE

<<First Name>> <<Last Name>>
VAR_DATA1
ADDRESS1
ADDRESS2
SEQ
CODE 2D CSZ BREAK
Ver ME COUNTRY

To Enroll, Please Call:
833-933-1098
Or Visit:
https://response.idx.us/health
Enrollment Code: <<XXXXXXXX>>

February 26, 2021

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

AllyAlign Health, Inc. ("AAH") is a Medicare Advantage special needs plan administrator headquartered in Richmond, Virginia. We are writing in order to inform you of an incident that may have exposed your sensitive personal information. We take the security of your personal information seriously and want to provide you with information and resources you can use to protect your information.

What Happened and What Information was Involved:

On November 14, 2020, AAH detected that it was the target of a cybersecurity attack. An unauthorized third party attempted to infiltrate the AAH's computer network, lock-out AAH, and then demand a ransom payment.

We have found no evidence that your information has been specifically accessed or acquired for misuse. However, due to the compromise of our network, we are notifying you of this incident. It is possible that the following information, if maintained by AAH, could have been exposed to the unauthorized third party: first and last name, mailing address, date of birth, social security number, Medicare Health Insurance Claim Number (HICN), Medicare Beneficiary Identifier (MBI), Medicaid recipient identification number (if applicable), medical claims history, health insurance policy number, and other medical information.

As of this writing, AAH has not received any reports of related identity theft since the date of the incident (November 14, 2020).

What We Are Doing:

Upon detecting this incident, we moved quickly to initiate a response, which included conducting an investigation with the assistance of IT specialists and confirming the security of our network environment. We have reviewed and altered our policies and procedures relating to the security of our systems and servers, as well as our information life cycle management.

We value the safety of your personal information and are therefore offering credit monitoring and identity theft protection services through IDX, a leading identity protection technology company. IDX's services include: at least 12 months of credit monitoring and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do:

We encourage you to contact IDX with any questions and to enroll in free IDX services by calling 1-833-933-1098 or going to https://response.idx.us/health and using the Enrollment Code provided above. IDX is available Monday through Friday 9 am – 9 pm Eastern Time. Please note the deadline to enroll is **May 26, 2021**.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Enclosed you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information.

For More Information:

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call IDX services at 1-833-933-1098, Monday through Friday 9 am – 9 pm Eastern Time.

AAH values the security of the personal data that we protect, and we apologize for any inconvenience that this incident has caused.

Sincerely,

David Crocker
Chief Information Officer

Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 www.transunion.com/credit-freeze

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (https://www.transunion.com/fraud-alerts); or
- Experian (https://www.experian.com/fraud/center.html).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: 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.

SEQ
CODE 2D

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 Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and 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 North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

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, and 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, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

AllyAlign Health
C/O IDX
PO Box 4129
Everett WA 98204

ENDORSE

<<First Name>> <<Last Name>>
VAR_DATA1
ADDRESS1
ADDRESS2
SEQ
CODE 2D CSZ BREAK
Ver PR COUNTRY

To Enroll, Please Call:
833-933-1098
Or Visit:
https://response.idx.us/health
Enrollment Code: <<XXXXXXXX>>

February 26, 2021

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

AllyAlign Health, Inc. ("AAH") is a Medicare Advantage special needs plan administrator headquartered in Richmond, Virginia. We are writing in order to inform you of an incident that may have exposed your sensitive personal information. We take the security of your personal information seriously and want to provide you with information and resources you can use to protect your information.

What Happened and What Information was Involved:

On November 14, 2020, AAH detected that it was the target of a cybersecurity attack. An unauthorized third party attempted to infiltrate the AAH's computer network, lock-out AAH, and then demand a ransom payment.

We have found no evidence that your information has been specifically accessed or acquired for misuse. However, due to the compromise of our network and out of an abundance of caution, we are notifying you of this incident. It is possible that the following information, if maintained by AAH, could have been exposed to the unauthorized third party: first and last name, mailing address, date of birth, social security number, Council for Affordable Quality Healthcare (CAQH) credentialing information (if applicable).

As of this writing, AAH has not received any reports of related identity theft since the date of the incident (November 14, 2020).

What We Are Doing:

Upon detecting this incident, we moved quickly to initiate a response, which included conducting an investigation with the assistance of IT specialists and confirming the security of our network environment. We have reviewed and altered our policies and procedures relating to the security of our systems and servers, as well as our information life cycle management.

We value the safety of your personal information and are therefore offering credit monitoring and identity theft protection services through IDX, a leading identity protection technology company. IDX's services include: at

least 12 months of credit monitoring and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do:

We encourage you to contact IDX with any questions and to enroll in free IDX services by calling 1-833-933-1098 or going to https://response.idx.us/health and using the Enrollment Code provided above. IDX is available Monday through Friday 9 am – 9 pm Eastern Time. Please note the deadline to enroll is **May 26, 2021**.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Enclosed you will find additional information regarding the resources available to you, and the steps that you can take to further protect your personal information.

For More Information:

We recognize that you may have questions not addressed in this letter. If you have additional questions, please call IDX services at 1-833-933-1098, Monday through Friday 9 am – 9 pm Eastern Time.

AAH values the security of the personal data that we protect, and we apologize for any inconvenience that this incident has caused.

Sincerely,

David Crocker
Chief Information Officer

Additional Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-800-909-8872 www.transunion.com/credit-freeze

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (https://www.transunion.com/fraud-alerts); or
- Experian (https://www.experian.com/fraud/center.html).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: 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 Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and 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 North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov.

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, and 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, and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.