Gregory Lederman
Office: (267) 930-4637
Fax: (267) 930-4771
Email: glederman@mullen.law

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

March 23, 2021

VIA E-MAIL

Office of the Attorney General of Iowa
Consumer Protection Division
Security Breach Notification
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
E-mail: consumer@ag.iowa.gov

Re: Notice of Data Event

Dear Sir or Madam:

We represent PACE Nebraska and PACE Iowa, doing business each, individually, as Immanuel Pathways ("Pathways"), located at 1044 North 115th Street, Omaha, Nebraska 68154, and are writing to notify your Office of an incident that may affect the security of some personal information relating to five hundred and seventy-eight (578) Iowa residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Pathways does not waive any rights or defenses regarding the applicability of Iowa law, the applicability of the Iowa data event notification statute, or personal jurisdiction.

Nature of the Data Event

Pathways serves as a provider of the Program of All-Inclusive Care for the Elderly ("PACE") to Iowa residents. PeakTPA provides third-party pharmacy administration services to Pathways program participants.

On January 23, 2021, Pathways received notice from PeakTPA of a ransomware incident. PeakTPA reported that on December 31, 2020, it experienced a ransomware event that resulted in the encryption of certain PeakTPA systems. PeakTPA reported that law enforcement was notified and that PeakTPA worked with forensic investigators to determine the nature and scope of the incident. Following its investigation, PeakTPA notified its customers that an unknown actor may have accessed or acquired certain PeakTPA customer data. PeakTPA reported that the data was accessed or exfiltrated by the threat actor at some point on or about December 29 and December 31, 2020.

Upon being notified by PeakTPA of the incident, Pathways immediately commenced an investigation to determine what, if any, sensitive Pathways participant information was potentially impacted. This investigation involved a review of the information provided by PeakTPA on January 27, 2021 to understand the scope of the incident. As a result of this incident, Pathways' investigation determined that the information potentially affected may have contained information including program names, dates of birth, Social Security numbers, Medicare identification numbers, and/or prescription information was involved.

Notice to Iowa Residents

On or about March 23, 2021, Pathways began providing written notice of this incident to affected individuals, which includes five hundred and seventy-eight (578) Iowa residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Pathways also posted notice of this incident on its website and provided notice to prominent media outlets in Iowa. A copy of the website notice is attached here as ***Exhibit B***. A copy of the media notice is attached here as ***Exhibit C***.

Other Steps Taken and To Be Taken

Upon discovering the event, Pathways moved quickly to investigate and respond to the incident, assess the security of internal Pathways systems, and identify potentially affected individuals in order to provide them with notice. Pathways is also working to review existing policies and procedures regarding its third-party vendors and working to evaluate additional measures and safeguards to protect against this type of incident in the future.

As an added precaution, Pathways is also providing complimentary access to three years of credit and identity monitoring services through Kroll, to individuals whose information was potentially affected by this incident, at no cost to these individuals.

Additionally, Pathways is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising 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 their Explanation of Benefits, account statements, and 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) 930-4637.

Very truly yours,

Gregory Lederman of
MULLEN COUGHLIN LLC

Exhibit A

PEAKTPA
Third Party Administration

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Please read this letter carefully. PeakTPA is writing to let you know about an incident involving some of your personal information. PeakTPA provides services to individuals like you ("participants") at Immanuel Pathways ("Pathways"), who are currently or were previously enrolled in the Program of All-Inclusive Care for the Elderly ("PACE"). Pathways gave us your information in order to participate in this PACE. We are writing to provide you with information about the event, to tell you what we have done, and steps you can take.

What Happened? On December 31, 2020, we became aware of unusual activity on our computers. During our investigation, we learned that certain information may have been accessed on or about December 29 and December 31, 2020. On January 23, 2021, we notified Pathways of this incident and that some current and former PACE participant information was possibly involved.

What Information Was Involved? On January 27, 2021, our investigation confirmed that some current and former Pathways participant information was involved, and we are notifying you now because our investigation confirmed that some of your information may also be involved. This information may include one or more of the following: full name, home address, date of birth, and Social Security number.

What We Are Doing. When we learned of this incident, we quickly took steps to secure our computers and began an investigation to determine what information was involved. Following the incident, we put into place additional security and are working with Pathways to make sure information related to Pathways participants is safe. We are also working to add more safety measures to protect information.

To prevent additional issues, we are also offering you free access to three years of identity monitoring services through Kroll. We encourage you to use these services, as we cannot act on your behalf. Please review the instructions in *Steps you Can Take to*

Help Protect Your Information, which is included in this letter, for additional information on these services.

What You Can Do. We encourage you to continue to look for signs of identity theft and fraud by reviewing your account statements and Explanation of Benefits. You can also review the enclosed *Steps you Can Take to Help Protect Your Information* for additional information on what you can do. You may also activate the free identity monitoring services we are offering.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **July 13, 2021** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

For More Information. If you have any questions about the incident that are not addressed in this letter, please call our dedicated assistance line Monday through Friday at 1-855-761-0196 between the hours of 8:00 a.m. to 5:30 p.m. Central Time. You may also write to PeakTPA at 345 Marshall Ave. Suite #101 St Louis, MO 63119.

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

Sincerely,

Michael McGarrigle
Senior Vice President, PeakTPA

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Credit Monitoring/Fraud Consultation/Identity Theft Restoration Services

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **July 13, 2021** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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. 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.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

This document includes an important notice. If you cannot read this attached document, please call 1-855-761-0196 for translation help.

TAGALOG

Ang liham na ito ay naglalaman ng mahalagang impormasyon. Kung hindi ninyo nababasa ang kalakip na liham, mangyaring tumawag sa 1-855-761-0196 upang magkaroon ng tulong sa pagsasalin sa Tagalog/Filipino.

RUSSIAN

В этомписьмесодержитсяважнаяинформация. ЕслиВынеможетепрочитатьприлагаемоеписьмо, позвонитепономеру 1-855-761-0196, и Вамбудутпредоставленыуслугипереводанарусскийязык.

KOREAN

이서신에는중요한정보가포함되어있습니다. 동봉된서신을읽으실수없으면
1-855-761-0196 로전화하여한국어번역지원을받으십시오.

ARMENIAN

Այս նամակը պարունակում է կարևոր տեղեկություններ: Եթե ներփակ նամակըչեք կարող կարդալ, խնդրվում է կապվեք 1-855-761-0196 հեռախոսահամարով, օգնություն ստանալՀայերեն լեզվով:

CHINESE

这封信包含了重要信息。如果您无法阅读随附的信件，请致电1-855-761-0196 寻求广东话翻译援助。

這封信包含了重要信息。如果您無法閱讀隨附的信件，請致電1-855-761-0196 尋求廣東話翻譯援助。

VIETNAMESE

Thư này bao hàm thông tin quan trọng. Nếu quý vị không đọc được thư đính kèm, vui lòng gọi 1-855-761-0196 để được giúp đỡ thông dịch trong tiếng Việt.

CHINESE

这封信包含了重要信息。如果您无法阅读随附的信件，请致电1-855-761-0196 寻求普通话翻译援助。

這封信包含了重要信息。如果您無法閱讀隨附的信件，請致電1-855-761-0196 尋求國語翻譯援助。

IRANIAN/PERSIAN

اینnامهحاوی اطلاعاتمهمی میباشد. اگرنامهضمیمهرانمیتوانیدبخوانید, لطفاًبرای کمکبهزبانفارسی باشمارهتلفن 1-855-761-0196–
.یگبسامتد

ARABIC

هذه الرسالة تحتوي علىء معلومات هامة .إذا لم تتمكن من قراءة الرسالة المرفقة، يرجى الاتصال علىء1-855-761-0196 للحصول علىء
.قدعاسم يفةمجرتلا ىلإ ةيبرعلا

Exhibit B

NOTICE OF DATA PRIVACY INCIDENT

PACE Nebraska, doing business in Nebraska as Immanuel Pathways, and PACE Iowa, doing business in Iowa as Immanuel Pathways, (each, individually, "Pathways"), provide notice of a recent incident at a third-party vendor, PeakTPA, that may affect the security of information for current and former participants enrolled in the Program of All-Inclusive Care for the Elderly ("PACE"). PeakTPA is a third-party administrator of certain PACE services and participant information was shared by Pathways to assist with this program. The confidentiality, privacy, and security of participant information is among one of Pathways' highest priorities, and Pathways takes this incident very seriously. Please know that to date, Pathways has not received any reports of actual or attempted misuse of participant information.

What Happened? On January 23, 2021, PeakTPA notified Pathways that on December 31, 2020, PeakTPA became aware of unusual activity involving their computers which resulted in the unauthorized access to certain participant information. Upon receiving notice of this incident, Pathways launched an investigation to find out what impact it may have on PACE participant information and to who that information belonged. During Pathways' investigation, PeakTPA reported that certain information of current or former PACE participants may have been accessed on or about December 29 and December 31, 2020. This incident did not involve internal Pathways' systems.

What Information Was Involved? On January 27, 2021, Pathways received additional information from PeakTPA which allowed Pathways to determine which current and former PACE participant information was involved. Pathways' investigation confirmed that certain current and former participant names, dates of birth, address, Medicare identification numbers, prescription information, and/or health insurance claim information was involved. In some cases, current and former participant Social Security numbers were also involved.

What We are Doing. PeakTPA is directly notifying the potentially impacted participants on behalf of Pathways and as an added precaution, is providing impacted participants with access to complementary credit monitoring and identity protection services. As part of its ongoing commitment to security of information in its care, Pathways is working to review its existing policies and procedures regarding third-party vendors and is working with PeakTPA to evaluate additional measures and security to protect against this type of incident in the future. Notice will also be provided to state and federal regulators, as required.

For More Information. You may have questions about this incident. If you have any additional questions and are impacted by this incident, please contact PeakTPA's dedicated assistance line at 855-761-0196 between the hours of 8:00 a.m. to 5:30 p.m. central time. You may also write to PeakTPA at 345 Marshall Ave. Suite #101. St Louis, MO 63119.

What You Can Do. Pathways encourages affected participants to remain vigilant against incidents of identity theft and fraud, to review Explanation of Benefits and account statements, and to monitor credit reports for suspicious activity. Under U.S. law consumers are entitled to one free credit report annually from each of the three major credit reporting bureaus. If you have further questions regarding your rights in relation to your credit report, please review the information contained in the letter that was mailed to you. If you are a participant and believe you may be impacted by this incident, you may also call 855-761-0196 for more information. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect personal information by contacting the consumer reporting bureaus below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Exhibit C

IMMANUEL PATHWAYS PROVIDES
NOTICE OF DATA PRIVACY INCIDENT

Omaha, Nebraska – March 23, 2021 – PACE Iowa, doing business as Immanuel Pathways ("Pathways"), provides notice of a recent incident at one of its third-party vendors, PeakTPA that may affect the security of information for current and former participants enrolled in the Program of All-Inclusive Care for the Elderly ("PACE") program. PeakTPA is a third-party administrator of certain PACE services and participant information was shared by Pathways to assist with this program. The confidentiality, privacy, and security of participant information is among one of Pathways' highest priorities, and Pathways takes this incident very seriously. Please know that to date, Pathways has not received any reports of actual or attempted misuse of participant information.

What Happened? On January 23, 2021, PeakTPA notified Pathways that on December 31, 2020, PeakTPA became aware of unusual activity involving their computers which resulted in the unauthorized access to certain participant information. Upon receiving notice of this incident, Pathways launched an investigation to find out what impact it may have on PACE participant information and to who that information belonged. During Pathways' investigation, PeakTPA reported that certain information of current or former PACE participants may have been accessed on or about December 29 and December 31, 2020. This incident did **not** involve internal Pathways' systems.

What Information Was Involved? On January 27, 2021, Pathways received additional information from PeakTPA which allowed Pathways to determine which current and former Pathways participant information was involved. Pathways' investigation confirmed that certain current and former participant names, dates of birth, Social Security numbers, Medicare identification numbers, and/or prescription information was involved.

What We are Doing. PeakTPA is directly notifying the potentially impacted program participants on behalf of Pathways and as an added precaution, is providing impacted participants with access to complementary credit monitoring and identity protection services. As part of its ongoing commitment to security of information in its care, Pathways is working to review its existing policies and procedures regarding third-party vendors and is working with PeakTPA to evaluate additional measures and security to protect against this type of incident in the future. Notice will also be provided to state and federal regulators, as required.

For More Information. Program participants who have been affected by this incident or who have further questions may contact PeakTPA at 1-855-761-0196. They may also write to PeakTPA at 345 Marshall Ave, Suite #101, St. Louis, MO 63119.

What You Can Do. Pathways encourages potentially affected participants to remain vigilant against incidents of identity theft and fraud, to review Explanation of Benefits and account statements, and to monitor credit reports for suspicious activity. Under U.S. law, consumers are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order this free credit report, consumers should visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also contact the three major credit bureaus directly to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit 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. Individuals who are victims of identity theft are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should an individual wish to place a fraud alert, they should contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in their name without their consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a security freeze, consumers will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the consumer's state Attorney General.