7825 3rd St N
Ste 105
Oakdale, MN 55128

10/29/2021

[redacted]

Dear [redacted]

I am writing on behalf of Viverant PT, LLC ("Viverant" or "we") to inform you about a data incident that involved your protected health information and/or personally identifiable information (collectively "Information"). On March 9, 2021, Viverant learned of a possible security incident that Viverant later confirmed occurred between February 23, 2021, and March 9, 2021. This letter provides you with information about this Incident, and as a precaution, provides steps you can take to protect your Information, though we are unaware of any misuse of your Information.

What Happened?

On March 9, 2021, we learned that suspicious emails were sent from an employee's email account (the "Incident"). Upon becoming aware of the Incident, we immediately investigated the matter and took measures to address and contain the Incident, including changing passwords, enacting stricter authentication requirements, employee trainings, and retaining national privacy and security experts. There is no indication that any Information was individually accessed or misused in any way.

Why Does Viverant Have My Information?

We provide physical therapy services to individuals across a number of states. As part of our normal business operations, we collected and utilized your Information to provide physical therapy services and collect payment for these services.

What Information Was Involved?

While we have no evidence of misuse of the Information, we determined that there may have been the following types of Information in the impacted mailbox: name, address, date of birth, social security number, driver's license number, medical record number, date of service, diagnostic or treatment information, credit/debit card number with password or security code, health insurance information, financial account number with or without password or routing number, medications, username with security questions and answers, vehicle identification number (VIN), and digital signature. Note that this describes general categories of Information involved in this Incident, and likely includes categories that are not relevant to you.

What We Are Doing.

Upon becoming aware of the Incident, we immediately implemented measures to further improve the security of our systems and practices. We worked with a leading privacy and security firm to aid in our investigation and response, and we are reporting this Incident to relevant government agencies.

What Can You Do?

It is always recommended that you regularly review account statements and report any suspicious activity to your child's financial institution. Please also review the enclosed "Additional Resources" section included with this letter, which describes additional steps you can take to help protect your child's Information.

For More Information.

If you have any questions about the Incident, please call 952-835-4512, Monday through Friday, from 9:00 a.m. to 5:00 p.m. Central (excluding some U.S. national holidays).

Sincerely

Dennis Cernohous
Chief Executive Officer

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

Do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, 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.

For Illinois residents: You may obtain information from the credit reporting agencies and the FTC about security freezes.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. As of September 18, 2018, when you place a fraud alert, it will last one year, instead of 90 days. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years. Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

7825 3rd St N
Ste 105
Oakdale, MN 55128

10/29/2021

[redacted]

Dear Parent or Guardian of [redacted]

I am writing on behalf of Viverant PT, LLC ("Viverant" or "we") to inform you about a data incident that involved your child's protected health information and/or personally identifiable information (collectively "Information"). On March 9, 2021, Viverant learned of a possible security incident that Viverant later confirmed occurred between February 23, 2021, and March 9, 2021. This letter provides you with information about this Incident, and as a precaution, provides steps you can take to protect your child's Information, though we are unaware of any misuse of your child's Information.

What Happened?

On March 9, 2021, we learned that suspicious emails were sent from an employee's email account (the "Incident"). Upon becoming aware of the Incident, we immediately investigated the matter and took measures to address and contain the Incident, including changing passwords, enacting stricter authentication requirements, employee trainings, and retaining national privacy and security experts. There is no indication that any Information was individually accessed or misused in any way.

Why Does Viverant Have My Information?

We provide physical therapy services to individuals across a number of states. As part of our normal business operations, we collected and utilized your child's Information to provide physical therapy services and collect payment for these services.

What Information Was Involved?

While we have no evidence of misuse of the Information, we determined that there may have been the following types of Information in the impacted mailbox: name, address, date of birth, social security number, driver's license number, medical record number, date of service, diagnostic or treatment information, credit/debit card number with password or security code, health insurance information, financial account number with or without password or routing number, medications, username with security questions and answers, vehicle identification number (VIN), and digital signature. Note that this describes general categories of information involved in this Incident, and likely includes categories that are not relevant to your child.

What We Are Doing.

Upon becoming aware of the Incident, we immediately implemented measures to further improve the security of our systems and practices. We worked with a leading privacy and security firm to aid in our investigation and response, and we are reporting this Incident to relevant government agencies.

What Can You Do?

It is always recommended that you regularly review account statements and report any suspicious activity to your child's financial institution. Please also review the enclosed "Additional Resources" section included with this letter, which describes additional steps you can take to help protect your child's Information.

For More Information.

If you have any questions about the Incident, please call 952-835-4512, Monday through Friday, from 9:00 a.m. to 5:00 p.m. Central (excluding some U.S. national holidays).

Sincerely

Dennis Cernohous
Chief Executive Officer

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

Do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, 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.

For Illinois residents: You may obtain information from the credit reporting agencies and the FTC about security freezes.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. As of September 18, 2018, when you place a fraud alert, it will last one year, instead of 90 days. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years. Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).