Notice of Vitra Data Security Incident

June (XX) 2023 - Vitra Health, Inc. (and Vitra Home Care, LLC (collectively, "Vitra"), a provider of services to Old Colony Elder Services ("OCES"), recently notified of a data security incident at Vitra involving the compromise of a Vitra employee email account.

Vitra took steps to directly notify impacted OCES clients of the incident via written letter between the dates of February 6, 2023 – May 21, 2023.

Vitra has provided the following information about the Incident:

"*Vitra discovered on December 8, 2022 that the email account was breached on December 6, 2022 in a phishing attack that targeted an employee's email account. Immediately, Vitra took action to prevent further breaches by disabling the compromised email, changing all credentials for the employee email account, confirming that no other emails had been breached, and initiating its internal investigation of the incident. Furthermore, Vitra retained a professional forensic investigator as well as a security and data privacy consultant to assist with investigating the breach. Vitra determined the email account that was improperly accessed contained information with various types of PHI, such as, name, address, date of birth, phone number, referral information, diagnoses, and Health Plan ID number. Vitra was able to confirm the information included in the breach did not include Social Security number, driver's license, or credit or debit card information.*

Consistent with its commitment to privacy, Vitra initiated several additional measures to reduce the risk of further breaches from occurring again. Immediate measures included expanding e-mail security, implementing new technical safeguards, and providing additional privacy and security training for our staff. As our ongoing commitment to the communities we serve, Vitra will continue to educate, train and monitor our staff competency on privacy and security matters, Vitra is already conducting a comprehensive review of our operations and IT systems, and retained professional outside assistance to perform HIPAA risk assessment."

Additional information about the Vitra data security incident is available at: Breach_Notification_Letter-Vitra_Health.pdf (vitrahealth.com). If you have any questions regarding this matter, you may contact the following toll-free number: 1-888-565-8027.

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	***Experian***	***TransUnion LLC***
P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/	P.O. Box 9554 Allen, TX 75013 https://www.experian.com/fraud/center.html (888) 397-3742	P.O. Box 6790 Fullerton, PA 92834-6790 https://www.transunion.com/fraud-alerts

(800) 525-6285 (800) 680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.equifax.com/personal/credit-report-services/credit-freeze/	http://experian.com/freeze	http://www.transunion.com/creditfreeze
1-800-349-9960	1-888-397-3742	1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added

to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

5. Protecting Your Medical Information.

The following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.