29245

[redacted]

Via First Class Mail

[redacted]

Dear [redacted]:

Vitra Health, Inc. ("Vitra") values and respects the privacy of your information, which is why we are writing to advise you of a recent cybersecurity incident that may impact the privacy of your personal information. While we have no reason to believe that your personal information has been misused for the purpose of committing fraud or identity theft, we are informing you so that you may take precautionary measures and we regret any concern it may cause you.

What Happened? On December 8, 2022, Vitra discovered that one of its employees' emails was compromised in a phishing attack on December 6, 2022. Vitra took immediate action to contain the incident by disabling the compromised email, changing all credentials for the applicable user, confirming no other emails had been jeopardized, and commencing its internal investigation of the incident. In addition, Vitra engaged a consultant to perform a forensic investigation of the compromise. On February 9, 2023, after a review of approximately 110,000 email messages and a manual review of over 18,000 images and 1,600 PDFs, 17 items were identified as containing personal information as defined under state data privacy law ("PI').

What Information was Involved? The documents that that included PI had name, address, driver's license number, and social security number.

What We Are Doing? Consistent with its commitment to privacy, Vitra initiated several additional measures to reduce the risk of future cybersecurity incidents. These measures included retaining professional outside assistance to perform a comprehensive risk assessment, expanding e-mail security, implementing new technical safeguards, and providing additional privacy and security training for our staff. Vitra will continue to educate, train and monitor our staff competency regarding privacy and security matters on an ongoing basis. Vitra is also notifying the Massachusetts Attorney General's Office and Massachusetts Office of the Consumer Affairs and Business Regulation about this incident, as required.

In addition, to help prevent possible misuse of your personal information, we will be offering a complimentary 24- month membership in the Equifax Complete Premier credit monitoring service ("Equifax"). To activate your Equifax membership and start monitoring your personal information, please follow the steps outlined on the last page of this enclosure.

What You Can Do. We do not have any indication that your personal information or any of your information has been used inappropriately. As a general protective measure, we encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for errors and suspicious activity. If you see charges or activity that you did not authorize, you should immediately contact the relevant financial institution or credit bureau reporting the activity. For more information on how you can protect yourself, please read the enclosed. [redacted]

For More Information. Again, we regret any concern or inconvenience this incident may cause [redacted]ave questions or concerns regarding this matter, please contact us at [redacted]om.
[redacted]

[redacted]

Sincerely,

Lawrence F. Christofori
Chief Financial Officer

Attachment 1

Under Massachusetts law, you have the right to obtain police reports, if any, that [redacted] filed regarding 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.

[redacted]rity freeze on your credit reports, free of charge. A security freeze prohibits [redacted]cy from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may [redacted]re with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

You should place your request for a security freeze with each of the three major credit reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com). For your convenience, we have included the contact information for these agencies below, and you may reach them via mail, online, or over the telephone.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-349-9960
https://www.equifax.com/personal/credit-report-services/

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
https://www.experian.com/freeze/center.html

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
https://www.transunion.com/credit-freeze

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so by mail, online, or by telephone:

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, the addresses where you have lived over the prior five years;

5. Proof of current address, such as a current utility bill, telephone bill, ren[redacted] or deed;

[redacted]egible photocopy of a government issued identification card (state driver's license or [redacted]ry identification, etc.);

[redacted]

7. Social Security Card, pay stub, or W2;

[redacted]

8. 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.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit reporting agencies must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, online, or by telephone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit reporting agencies have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, online, or by telephone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

Credit Reports: In order to determine whether any unauthorized credit was obtained with your personal information, you may obtain a copy of your credit report, free of charge, once every 12 months from each of the three major credit reporting agencies by visiting www.annualcreditreport.com or by call toll free at (877) 322-8228.

Fraud Alerts: You may also request information on how to place a fraud alert by contacting any of the above credit reporting agencies. A fraud alert is intended to alert you if someone attempts to obtain credit in your name without your consent. It is recommended that you remain vigilant for any incidents of fraud or identity theft by reviewing credit card account statements and your credit report for unauthorized activity. You may also contact the Federal Trade Commission ("FTC") to learn more about how to prevent identity theft: [redacted]

FTC, Consumer Response Center
[redacted]ennsylvania Ave., NW
[redacted].C. 20590
[redacted]cp/edu/microsites/idtheft
877-IDTHEFT (438-4338)
[redacted]

<First Name> <Last Name>
Enter your Activation Code: [redacted]
Enrollment Deadline: **<Expiration Date>**

[redacted]

Equifax Complete™ Premier

[redacted]8 with a credit file to take advantage of the product

Key Features

- [redacted]s to your 3-bureau credit report and VantageScore[1] credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring[2] with email notifications of key changes to your credit reports
- WebScan notifications[3] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[4], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[5]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[6].
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of 321339694520 **<Activation Code>** then click "Submit"

1. **Register**:
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account**:
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity**:
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1] The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Anyone-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

[2] Credit monitoring from Experian and TransUnion will take several days to begin.

[3] WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

[4] The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

[5] Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com

[6] The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

[redacted]

Via First Class Mail

[redacted]

Dear [redacted]

Vitra Health, Inc. ("Vitra") values and respects the privacy of your information, which is why we are writing to advise you of a recent cybersecurity incident that may impact the privacy of your personal information. While we have no reason to believe that your personal information has been misused for the purpose of committing fraud or identity theft, we are informing you so that you may take precautionary measures and we regret any concern it may cause you.

What Happened? On December 8, 2022, Vitra discovered that one of its employees' emails was compromised in a phishing attack on December 6, 2022. Vitra took immediate action to contain the incident by disabling the compromised email, changing all credentials for the applicable user, confirming no other emails had been jeopardized, and commencing its internal investigation of the incident. In addition, Vitra engaged a consultant to perform a forensic investigation of the compromise. On February 9, 2023, after a review of approximately 110,000 email messages and a manual review of over 18,000 images and 1,600 PDFs, 17 items were identified as containing personal information as defined under state data privacy law ("PI').

What Information was Involved? The documents that that included PI had name, address, and driver's license number.

What We Are Doing? Consistent with its commitment to privacy, Vitra initiated several additional measures to reduce the risk of future cybersecurity incidents. These measures included retaining professional outside assistance to perform a comprehensive risk assessment, expanding e-mail security, implementing new technical safeguards, and providing additional privacy and security training for our staff. Vitra will continue to educate, train and monitor our staff competency regarding privacy and security matters on an ongoing basis. Vitra is also notifying the Massachusetts Attorney General's Office and Massachusetts Office of the Consumer Affairs and Business Regulation about this incident, as required.

What You Can Do. We do not have any indication that your personal information or any of your information has been used inappropriately. As a general protective measure, we encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for errors and suspicious activity. If you see charges or activity that you did not authorize, you should immediately contact the relevant financial institution or credit bureau reporting the activity. For more information on how you can protect yourself, please read the enclosed.

Attachment 1

Under Massachusetts law, you have the right to obtain police reports, if any, that may have been filed regarding 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.

You may place a security freeze on your credit reports, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

You should place your request for a security freeze with each of the three major credit reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com). For your convenience, we have included the contact information for these agencies below, and you may reach them via mail, online, or over the telephone.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-349-9960
https://www.equifax.com/personal/credit-report-services/

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
https://www.experian.com/freeze/center.html

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
https://www.transunion.com/credit-freeze

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so by mail, online, or by telephone:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);

2. Social Security Number;

3. Date of birth;

For More Information. Again, we regret any concern or inconvenience this incident may cause you. If you have questions or concerns regarding this matter, please contact us at support@vitrahealth.com.

Sincerely,

Lawrence F. Christofori

Chief Financial Officer

4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;

5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;

6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);

7. Social Security Card, pay stub, or W2;

8. 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.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit reporting agencies must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, online, or by telephone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit reporting agencies have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, online, or by telephone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

Credit Reports: In order to determine whether any unauthorized credit was obtained with your personal information, you may obtain a copy of your credit report, free of charge, once every 12 months from each of the three major credit reporting agencies by visiting www.annualcreditreport.com or by call toll free at (877) 322-8228.

Fraud Alerts: You may also request information on how to place a fraud alert by contacting any of the above credit reporting agencies. A fraud alert is intended to alert you if someone attempts to obtain credit in your name without your consent. It is recommended that you remain vigilant for any incidents of fraud or identity theft by reviewing credit card account statements and your credit report for unauthorized activity. You may also contact the Federal Trade Commission ("FTC") to learn more about how to prevent identity theft:

FTC, Consumer Response Center
600 Pennsylvania Ave., NW
Washington D.C. 20590
www.ftc.gov/bcp/edu/microsites/idtheft
877-IDTHEFT (438-4338)