23452

Ivy Dental Care, PLLC
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

[redacted]

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

[redacted]

Dear [redacted]:

We are writing with important information regarding a security incident. The privacy and security of the personal information we maintain is of the utmost importance to Ivy Dental Care. We wanted to provide you with information about the incident and let you know that we continue to take significant measures to protect your information.

What Happened?

On April 24, 2021, we became aware of a cybersecurity incident that infected a number of our systems and encrypted files on several machines. We cleared the malware from our systems, and restored data and functionality.

What We Are Doing.

Upon learning of the issue, in addition to taking the remediation and restoration steps above, we commenced an immediate and thorough investigation. As part of our investigation, we engaged external cybersecurity professionals experienced in handling these types of incidents.

Our investigation concluded that an unauthorized party removed a limited number of files and folders from our system. Following the conclusion of the forensic investigation, we performed a comprehensive manual document review to identify what information might have been present in those files. At the conclusion of the manual review, we concluded on August 23, 2021 that certain elements of your protected health information were present in certain impacted files. While we have no indication or evidence that any of that data has been or will be misused, we thought it important to notify you of this incident.

Cybersecurity attacks against healthcare providers are becoming more and more common, particularly since the COVID-19 pandemic began. Although we have protections in place to prevent this type of attack from happening, attackers have been increasingly successful in penetrating the networks of providers who have security measures in place. After discovering the incident, we immediately notified the San Antonio Police Department as well as the FBI. Additionally, since the incident we have worked with our Information Technology ("IT") managed services provider to implement additional security measures in an effort to prevent a similar event from occurring in the future.

What Information Was Involved?

The accessed files contained some of your personal information, specifically your [redacted].

What You Can Do.

We have no reason to believe that your information has been or will be misused. Nevertheless, to protect you from potential misuse of your information, we are offering a complimentary two-year membership in Equifax® Credit Watch™ Gold. Equifax® Credit Watch™ Gold is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and Equifax® Credit Watch™ Gold, including instructions on how to activate your complimentary two-year membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. We are also offering steps you can take to protect your medical information on the following pages.

For More Information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at 866-211-0774. Please be sure to call this number to ensure the fastest response to any questions you may have regarding the incident. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 8am – 8pm Central Time.

Please accept our apologies that this incident occurred and please know we are committed to maintaining the privacy of personal information in our possession. It has been a pleasure for the team at Ivy Dental Care to work with each and every one of our patients and we sincerely look forward to seeing you and your family in our office soon.

Sincerely,

Ivy Dental Care

EQUIFAX®

Enter your Activation Code: [redacted]
Enrollment Deadline: [redacted]

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] 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[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- 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[4]

Enrollment Instructions

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

Enter your unique Activation Code of [redacted] then click "Submit" and follow these 4 steps:

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]*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.* [2]*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.* [3]*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* [4]*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.*

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary two-year credit monitoring services, we recommend that you place an initial one (1) 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
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion LLC
P.O. Box 6790
Fullerton, PA 92834-6790
https://www.transunion.com/fraud-alerts
(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
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(800) 349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
(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.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

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.**

We have no evidence that your medical information involved in this incident was or will be used for any unintended purposes. However, to protect against medical identity theft, we recommend that you:

- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company for any items you do not recognize.
- 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.
- 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 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."

Ivy Dental Care, PLLC
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

[redacted]
To the Parent or Guardian of:
[redacted]

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

[redacted]

Dear Parent or Guardian of [redacted]:

We are writing with important information regarding a security incident. The privacy and security of the personal information we maintain is of the utmost importance to Ivy Dental Care. We wanted to provide you with information about the incident and let you know that we continue to take significant measures to protect your minor's information.

What Happened?

On April 24, 2021, we became aware of a cybersecurity incident that infected a number of our systems and encrypted files on several machines. We cleared the malware from our systems, and restored data and functionality.

What We Are Doing.

Upon learning of the issue, in addition to taking the remediation and restoration steps above, we commenced an immediate and thorough investigation. As part of our investigation, we engaged external cybersecurity professionals experienced in handling these types of incidents.

Our investigation concluded that an unauthorized party removed a limited number of files and folders from our system. Following the conclusion of the forensic investigation, we performed a comprehensive manual document review to identify what information might have been present in those files. At the conclusion of the manual review, we concluded on August 23, 2021 that certain elements of your minor's protected health information were present in certain impacted files. While we have no indication or evidence that any of that data has been or will be misused, we thought it important to notify you of this incident.

Cybersecurity attacks against healthcare providers are becoming more and more common, particularly since the COVID-19 pandemic began. Although we have protections in place to prevent this type of attack from happening, attackers have been increasingly successful in penetrating the networks of providers who have security measures in place. After discovering the incident, we immediately notified the San Antonio Police Department as well as the FBI. Additionally, since the incident we have worked with our Information Technology ("IT") managed services provider to implement additional security measures in an effort to prevent a similar event from occurring in the future.

What Information Was Involved?

The accessed files contained some of your minor's personal information, specifically your minor's [redacted].

What You Can Do.

We have no reason to believe that your minor's information has been or will be misused. Nevertheless, we encourage you to activate the two-year complimentary membership in Equifax® child monitoring. For more information on identity theft prevention and Equifax® child monitoring, including instructions on how to activate your complimentary two-year membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your minor's personal information, including placing a fraud alert and/or security freeze on your minor's credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. We are also offering steps you can take to protect your minor's medical information on the following pages.

For More Information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at 866-211-0774. Please be sure to call this number to ensure the fastest response to any questions you may have regarding the incident. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 8am – 8pm Central Time.

Please accept our apologies that this incident occurred and please know we are committed to maintaining the privacy of personal information in our possession. It has been a pleasure for the team at Ivy Dental Care to work with each and every one of our patients and we sincerely look forward to seeing you and your family in our office soon.

Sincerely,

Ivy Dental Care

EQUIFAX®

Enter your Activation Code [redacted]
Enrollment Deadline: [redacted]

Equifax Child Monitoring Package

Key Features

- Child Monitoring for up to four children under the age of 18
- Emailed notifications to the primary adult member of activity on the child's Equifax credit report

Enrollment Instructions

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

Enter your unique Activation Code of [redacted] then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with parent/guardian 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 parent/guardian email address, create a password, and to 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 parent/guardian identity, you will see the Checkout Page. Click 'Sign Me Up' to finish enrolling.
   The confirmation page shows parent/guardian completed enrollment.
   Click "View My Product" to access the product features and enroll minor children.

How to Add Minors to Your Equifax Child Monitoring Package

You will be able to add minors to your Equifax Child Monitoring Package through your product dashboard.

1. Sign in to your account to access the "Your People" module on your dashboard.
2. Click the link to "Add a Child"
3. From there, enter your child's first name, last name, date of birth and social security number.
   Repeat steps for each minor child (up to four)

Equifax will then create an Equifax credit file for your child, lock it and then alert you if there is any activity on that child's Equifax credit file. You can add up to 4 children under the age of 18 with your Equifax Child Monitoring Package.

– OTHER IMPORTANT INFORMATION –

1. **Placing a Fraud Alert on Your Minor's Credit File.**

We recommend that you place an initial 12 month "fraud alert" on your minor's credit files (if one exists), 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
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion LLC
P.O. Box 6790
Fullerton, PA 92834-6790
https://www.transunion.com/fraud-alerts
(800) 680-7289

2. Consider Placing a Security Freeze on Your Minor's Credit File.

If you are very concerned about your minor becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your minor's credit file (if one exists), at no cost to you. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your minor's credit report or any information from it without your express authorization. You may place a security freeze on your minor's credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

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

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/securityfreeze
(888) 909-8872

In order to place the security freeze, you'll need to supply your minor's name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit monitoring 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 minor's personal information has been used to file a false tax return, to open an account or to attempt to open an account in your minor's name or to commit fraud or other crimes against your minor, 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 minor's free credit reports online at www.annualcreditreport.com. Once you receive your minor's 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 minor's initial credit reports, the Federal Trade Commission (FTC) recommends that you check your minor's credit reports periodically. Checking your minor's credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your minor's credit reports or have reason to believe your minor's 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 your minor 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 minor's 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.

If this notice letter states that your minor's financial account information and/or credit or debit card information was impacted, we recommend that you contact your minor's financial institution to inquire about steps to take to protect your minor's account, including whether you should close your minor's account or obtain a new account number.

5. Protecting Your Minor's Medical Information.

We have no evidence that your minor's medical information involved in this incident was or will be used for any unintended purposes. However, to protect against medical identity theft, we recommend that you:

- Only share your minor's health insurance cards with your minor's health care providers and other family members who are covered under your minor's insurance plan or who help you with your minor's medical care.
- Review your minor's "explanation of benefits statement" which you receive from your minor's health insurance company. Follow up with your minor's insurance company for any items you do not recognize.
- Ask your minor's insurance company for a current year-to-date report of all services paid for your minor as a beneficiary. Follow up with your minor's insurance company 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."