



August 27, 2020

Robert Walker
601.499.8083 (direct)
Robert.Walker@wilsonelser.com

Via First Class Mail

Attorney General Gordon J. MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

RECEIVED

SEP 08 2020

Re: Data Security Incident

CONSUMER PROTECTION

Dear Attorney General MacDonald:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Utah Pathology Services, Inc. ("Utah Pathology") with respect to a potential data security incident described in more detail below. Utah Pathology takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

1. Nature of the security Incident.

On June 30, 2020 Utah Pathology discovered that an unknown party attempted to redirect funds within Utah Pathology. This suspicious activity did not involve any patient information. Upon discovery of the attempted fraud, Utah Pathology quickly secured the impacted email account and launched an investigation. The investigation was performed with the help of independent IT security and forensic investigators to determine the scope and extent of the potential unauthorized access to Utah Pathology systems and any sensitive information.

2. Number of New Hampshire residents affected.

On or about August 18, 2020, Utah Pathology finished identifying a population of five (5) New Hampshire residents that were potentially affected by this Incident. Incident notification letters addressed to that individual will be mailed on August 28, 2020, via First Class Mail. A sample copy of the Incident notification letter being mailed to potentially affected residents of New Hampshire is included with this letter at **Exhibit A**.

3. Steps taken.

Utah Pathology takes the security of all information in our control very seriously, and are taking steps to prevent a similar event from occurring in the future by implementing additional safeguards and security measures to enhance the privacy and security of information in our systems. Utah Pathology also reported this incident to law enforcement.

1400 Meadowbrook Road, Suite 100 • Jackson, MS 39211 • p 601.499.8077 • f 601.499.8078

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

5819600v.1

Utah Pathology has also gone to great lengths to identify and notify any individuals who were potentially impacted as result of this Incident including the hiring of a third-party vendor to arrange for any potentially affected residents of New Hampshire to receive complimentary credit monitoring and identify theft protection services for twelve (12) months.

4. Contact information.

Utah Pathology remains dedicated to protecting the sensitive information within its control. If you have any questions or need additional information, please do not hesitate to contact me at Robert.Walker@wilsonelser.com or (601) 499-8083.

Very truly yours,



Robert Walker



EXHIBIT A



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

Subject: Notification of Data Security Incident

Dear <<Name 1>>:

We are writing to inform you of a data security incident involving Utah Pathology Services, Inc. ("Utah Pathology") that may have resulted in the unauthorized access to some of your personal information. We take the privacy and protection of your personal information very seriously. We sincerely apologize and regret any inconvenience this incident may cause. This letter contains information about what happened, steps we have taken, and the resources we are making available to you to protect your identity.

On June 30, 2020, we learned that an unknown party attempted to redirect funds within Utah Pathology. This suspicious activity did not involve any patient information. Upon discovery of the attempted fraud, Utah Pathology quickly secured the impacted email account and launched an investigation. The investigation was performed with the help of independent IT security and forensic investigators to determine the scope and extent of the potential unauthorized access to Utah Pathology systems and any sensitive information.

Our investigation is ongoing, but we discovered that your personal information, including your name and one or more of the following personal attributes was accessible to the unauthorized party: your date of birth, gender, phone number, mailing address, email address, insurance information including ID and group numbers, and medical and health information including internal record numbers and clinical and diagnostic information related to pathology services. At this time we do not have any evidence that any patient information has been misused. Nevertheless, we are notifying all potentially affected patients out of an abundance of caution.

Although we are unaware of any misuse of our or anyone's information, to help relieve concerns and restore confidence following this incident, we have secured the services of CyberScout to provide identity monitoring, at no cost to you, for twelve (12) months.

Single-Bureau Credit Monitoring
+ Proactive Fraud Assistance +
ID Theft and Fraud Resolution +
Credit Freeze

DBC P20 B109

We are providing you with access to **Single Bureau Credit Monitoring** services at no charge. Services are for one year from the date of enrollment. When changes occur to your Experian credit file, notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud you will also have access remediation support from a CyberScout Fraud Investigator. In order for you to receive the monitoring service described above, you must enroll within 90 days from the date of this letter.


How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to <https://www.myidmanager.com> and follow the instructions provided. When prompted please provide the following unique code to receive services: <<**Activation Code**>>. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

We take the security of all information in our control very seriously, and are taking steps to prevent a similar event from occurring in the future by implementing additional safeguards and security measures to enhance the privacy and security of information in our systems. We also reported this incident to law enforcement.

Please know that the protection and security of your personal information is of our outmost priority, and we sincerely regret any concern or inconvenience that this matter may cause you. If you have any questions, please call 855-917-3569 Monday through Friday, 7 am to 7 pm Mountain Time.

Sincerely,



Dennem Wolfley
Chief Operating Officer
Utah Pathology Services, Inc.

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Arizona, Colorado, Maryland, Rhode Island, Illinois, New York, and North Carolina:

You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

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

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

New York Office of the Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224, 1-800-771-7755, <https://ag.ny.gov/consumer-frauds/identity-theft>

Colorado Office of the Attorney General Consumer Protection, 1300 Broadway, 9th Floor, Denver, CO 80203, 1-720-508-6000, www.coag.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004, 1-602-542-5025

Illinois Office of the Attorney General Consumer Protection Division, 100 W Randolph St., Chicago, IL 60601, 1-800-243-0618, www.illinoisattorneygeneral.gov

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed

below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

800-525-6285

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

www.experian.com/freeze

888-397-3742

TransUnion (FVAD)

P.O. Box 2000

Chester, PA 19022

freeze.transunion.com

800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

Subject: Notification of Data Security Incident

Dear <<Name 1>>:

We are writing to inform you of a data security incident involving Utah Pathology Services, Inc. ("Utah Pathology") that may have resulted in the unauthorized access to some of your personal information. We take the privacy and protection of your personal information very seriously. We sincerely apologize and regret any inconvenience this incident may cause. This letter contains information about what happened, steps we have taken, and the resources we are making available to you to protect your identity.

On June 30, 2020, we learned that an unknown party attempted to redirect funds within Utah Pathology. This suspicious activity did not involve any patient information. Upon discovery of the attempted fraud, Utah Pathology quickly secured the impacted email account and launched an investigation. The investigation was performed with the help of independent IT security and forensic investigators to determine the scope and extent of the potential unauthorized access to Utah Pathology systems and any sensitive information.

Our investigation is ongoing, but we discovered that your personal information, including your name and one or more of the following personal attributes was accessible to the unauthorized party: your date of birth, gender, phone number, mailing address, email address, insurance information including ID and group numbers, medical and health information including internal record numbers and clinical and diagnostic information related to pathology services, and Social Security number. At this time we do not have any evidence that any patient information has been misused. Nevertheless, we are notifying all potentially affected patients out of an abundance of caution.

Although we are unaware of any misuse of our or anyone's information, to help relieve concerns and restore confidence following this incident, we have secured the services of CyberScout to provide identity monitoring, at no cost to you, for twelve (12) months.

Single-Bureau Credit Monitoring
+ Proactive Fraud Assistance +
ID Theft and Fraud Resolution +
Credit Freeze

DBC P20 B109

We are providing you with access to **Single Bureau Credit Monitoring** services at no charge. Services are for one year from the date of enrollment. When changes occur to your Experian credit file, notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions you might have. In the event you become a victim of fraud you will also have access remediation support from a CyberScout Fraud Investigator. In order for you to receive the monitoring service described above, you must enroll within 90 days from the date of this letter.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to <https://www.myidmanager.com> and follow the instructions provided. When prompted please provide the following unique code to receive services: <<**Activation Code**>>. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

We take the security of all information in our control very seriously, and are taking steps to prevent a similar event from occurring in the future by implementing additional safeguards and security measures to enhance the privacy and security of information in our systems. We also reported this incident to law enforcement.

Please know that the protection and security of your personal information is of our outmost priority, and we sincerely regret any concern or inconvenience that this matter may cause you. If you have any questions, please call 855-917-3569 Monday through Friday, 7 am to 7 pm Mountain Time.

Sincerely,

Dennem Wolfley

Dennem Wolfley
Chief Operating Officer
Utah Pathology Services, Inc.

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Arizona, Colorado, Maryland, Rhode Island, Illinois, New York, and North Carolina:

You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

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

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224, 1-800-771-7755, <https://ag.ny.gov/consumer-frauds/identity-theft>

Colorado Office of the Attorney General Consumer Protection, 1300 Broadway, 9th Floor, Denver, CO 80203, 1-720-508-6000, www.coag.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004, 1-602-542-5025

Illinois Office of the Attorney General Consumer Protection Division, 100 W Randolph St., Chicago, IL 60601, 1-800-243-0618, www.illinoisattorneygeneral.gov

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed

below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

800-525-6285

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

www.experian.com/freeze

888-397-3742

TransUnion (FVAD)

P.O. Box 2000

Chester, PA 19022

freeze.transunion.com

800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>

To the Parent or Guardian of

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

Subject: Notification of Data Security Incident

Dear Parent or Guardian of <<Name 1>>:

We are writing to inform you of a data security incident involving Utah Pathology Services, Inc. ("Utah Pathology") that may have resulted in the unauthorized access to some of your dependent's personal information. We take the privacy and protection of your dependent's personal information very seriously. We sincerely apologize and regret any inconvenience this incident may cause. This letter contains information about what happened, steps we have taken, and the resources we are making available to you to protect your identity.

On June 30, 2020, we learned that an unknown party attempted to redirect funds within Utah Pathology. This suspicious activity did not involve any patient information. Upon discovery of the attempted fraud, Utah Pathology quickly secured the impacted email account and launched an investigation. The investigation was performed with the help of independent IT security and forensic investigators to determine the scope and extent of the potential unauthorized access to Utah Pathology systems and any sensitive information.

Our investigation is ongoing, but we discovered that your dependent's personal information, including their name and one or more of the following personal attributes was accessible to the unauthorized party: date of birth, gender, phone number, mailing address, email address, insurance information including ID and group numbers, and medical and health information including internal record numbers and clinical and diagnostic information related to pathology services. At this time we do not have any evidence that any patient information has been misused. Nevertheless, we are notifying all potentially affected patients out of an abundance of caution.

Although we are unaware of any misuse of our or anyone's information, to help relieve concerns and restore confidence following this incident, we have secured the services of Equifax to provide your dependent with complimentary identity monitoring services. Information about the services being provided by Equifax, along with additional information about how to protect yourself, is included in the materials attached to this letter.

We take the security of all information in our control very seriously, and are taking steps to prevent a similar event from occurring in the future by implementing additional safeguards and security measures to enhance the privacy and security of information in our systems. We also reported this incident to law enforcement.

Please know that the protection and security of your dependent's personal information is of our outmost priority, and we sincerely regret any concern or inconvenience that this matter may cause you. If you have any questions, please call 855-917-3569 Monday through Friday, 7 am to 7 pm Mountain Time.

Sincerely,

Dennem Wolfley
Chief Operating Officer
Utah Pathology Services, Inc.



Enter your Activation Code: <<ACTIVATION CODE>>

Product Information

Equifax Child Identity Monitoring will scan the Equifax credit database for any instances of the minor's social security number and look for a copy of the minor's Equifax credit file.

- If no SSN match is found and no Equifax credit file exists, Equifax will create an Equifax credit file in the minor's name and immediately "lock" the Equifax credit file. This will prevent access to the minor's Equifax credit file in the future. If Equifax receives a request for your minor's Equifax credit report, you will receive an email alert.
- If there is a match and an Equifax credit file exists, Equifax will immediately "lock" the file and alert you to activity against the file, such as an attempt to open a new line of credit.
- The minor's Equifax credit file will be locked for 12 months from date of activation. After that time, the minor's Equifax credit file will be deleted from our credit database if it contains no credit data.

Enrollment Instructions

To enroll in Equifax Child Identity Monitoring go to http://myservices.equifax.com/efx1_brminor and follow the instructions below:

1. **Welcome Page:** Enter the Activation Code provided at the top of this page in the "Activation Code" box and click the "Submit" button.
2. **Register:** Complete the form with **YOUR** contact information first (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.
3. **Create Account:** Complete the form with your email address, create a User Name and Password, after reviewing the Terms of Use, check the box to accept the Terms of Use and click the "Continue" button.
4. **Verify ID:** The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.
5. **Order Confirmation:** This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.
6. **Click the orange button "Enroll Child"** to enter your child's information (child's name, Date of Birth and Social Security Number). Note: if you enter the child's SSN incorrectly, you will need to remove the minor by going to your Member Center and clicking on "My Account" to remove the minor from the account. You may then re-enroll the minor with the correct SSN.
7. **Check the box confirming you are the child's parent or guardian.**
8. **Click "Submit"** to enroll your child.

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Arizona, Colorado, Maryland, Rhode Island, Illinois, New York, and North Carolina:

You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

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

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

New York Office of the Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224, 1-800-771-7755, <https://ag.ny.gov/consumer-frauds/identity-theft>

Colorado Office of the Attorney General Consumer Protection, 1300 Broadway, 9th Floor, Denver, CO 80203, 1-720-508-6000, www.coag.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004, 1-602-542-5025

Illinois Office of the Attorney General Consumer Protection Division, 100 W Randolph St., Chicago, IL 60601, 1-800-243-0618, www.illinoisattorneygeneral.gov

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed

below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

800-525-6285

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

www.experian.com/freeze

888-397-3742

TransUnion (FVAD)

P.O. Box 2000

Chester, PA 19022

freeze.transunion.com

800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>

To the Parent or Guardian of

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<Date>>

<<City>><<State>><<Zip>>

<<Country>>

Subject: Notification of Data Security Incident

Dear Parent or Guardian of <<Name 1>>:

We are writing to inform you of a data security incident involving Utah Pathology Services, Inc. ("Utah Pathology") that may have resulted in the unauthorized access to some of your dependent's personal information. We take the privacy and protection of your dependent's personal information very seriously. We sincerely apologize and regret any inconvenience this incident may cause. This letter contains information about what happened, steps we have taken, and the resources we are making available to you to protect your identity.

On June 30, 2020, we learned that an unknown party attempted to redirect funds within Utah Pathology. This suspicious activity did not involve any patient information. Upon discovery of the attempted fraud, Utah Pathology quickly secured the impacted email account and launched an investigation. The investigation was performed with the help of independent IT security and forensic investigators to determine the scope and extent of the potential unauthorized access to Utah Pathology systems and any sensitive information.

Our investigation is ongoing, but we discovered that your dependent's personal information, including their name and one or more of the following personal attributes was accessible to the unauthorized party: date of birth, gender, phone number, mailing address, email address, insurance information including ID and group numbers, medical and health information including internal record numbers and clinical and diagnostic information related to pathology services, and Social Security number. At this time we do not have any evidence that any patient information has been misused. Nevertheless, we are notifying all potentially affected patients out of an abundance of caution.

Although we are unaware of any misuse of our or anyone's information, to help relieve concerns and restore confidence following this incident, we have secured the services of Equifax to provide your dependent with complimentary identity monitoring services. Information about the services being provided by Equifax, along with additional information about how to protect yourself, is included in the materials attached to this letter.

We take the security of all information in our control very seriously, and are taking steps to prevent a similar event from occurring in the future by implementing additional safeguards and security measures to enhance the privacy and security of information in our systems. We also reported this incident to law enforcement.

Please know that the protection and security of your dependent's personal information is of our outmost priority, and we sincerely regret any concern or inconvenience that this matter may cause you. If you have any questions, please call 855-917-3569 Monday through Friday, 7 am to 7 pm Mountain Time.

Sincerely,

Dennem Wolfley
Chief Operating Officer
Utah Pathology Services, Inc.



Enter your Activation Code: <<ACTIVATION CODE>>

Product Information

Equifax Child Identity Monitoring will scan the Equifax credit database for any instances of the minor's social security number and look for a copy of the minor's Equifax credit file.

- If no SSN match is found and no Equifax credit file exists, Equifax will create an Equifax credit file in the minor's name and immediately "lock" the Equifax credit file. This will prevent access to the minor's Equifax credit file in the future. If Equifax receives a request for your minor's Equifax credit report, you will receive an email alert.
- If there is a match and an Equifax credit file exists, Equifax will immediately "lock" the file and alert you to activity against the file, such as an attempt to open a new line of credit.
- The minor's Equifax credit file will be locked for 12 months from date of activation. After that time, the minor's Equifax credit file will be deleted from our credit database if it contains no credit data.

Enrollment Instructions

To enroll in Equifax Child Identity Monitoring go to http://myservices.equifax.com/efx1_brminor and follow the instructions below:

1. **Welcome Page:** Enter the Activation Code provided at the top of this page in the "Activation Code" box and click the "Submit" button.
2. **Register:** Complete the form with **YOUR** contact information first (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.
3. **Create Account:** Complete the form with your email address, create a User Name and Password, after reviewing the Terms of Use, check the box to accept the Terms of Use and click the "Continue" button.
4. **Verify ID:** The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.
5. **Order Confirmation:** This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.
6. **Click the orange button "Enroll Child"** to enter your child's information (child's name, Date of Birth and Social Security Number). Note: if you enter the child's SSN incorrectly, you will need to remove the minor by going to your Member Center and clicking on "My Account" to remove the minor from the account. You may then re-enroll the minor with the correct SSN.
7. **Check the box confirming you are the child's parent or guardian.**
8. **Click "Submit"** to enroll your child.

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon:

State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Arizona, Colorado, Maryland, Rhode Island, Illinois, New York, and North Carolina:

You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

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

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224, 1-800-771-7755, <https://ag.ny.gov/consumer-frauds/identity-theft>

Colorado Office of the Attorney General Consumer Protection, 1300 Broadway, 9th Floor, Denver, CO 80203, 1-720-508-6000, www.coag.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004, 1-602-542-5025

Illinois Office of the Attorney General Consumer Protection Division, 100 W Randolph St., Chicago, IL 60601, 1-800-243-0618, www.illinoisattorneygeneral.gov

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed

below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

800-525-6285

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

www.experian.com/freeze

888-397-3742

TransUnion (FVAD)

P.O. Box 2000

Chester, PA 19022

freeze.transunion.com

800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.