November 3, 2020

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via E-MAIL

Attorney General Tom Miller
Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
consumer@ag.iowa.gov

Re: Data Security Incident

Dear Attorney General Miller:

We represent Cedar Falls Community School District ("Cedar Falls CSD") regarding a data security incident involving Timberline Billing Services, LLC ("Timberline"), a company located in Iowa. Cedar Falls CSD is located in Cedar Falls, Iowa. Timberline provides Medicaid reimbursement billing services for Medicaid eligible students on behalf of 190 school districts in Iowa, including Cedar Falls CSD. Cedar Falls CSD takes the security and privacy of the information in its control seriously, and is working with Timberline to prevent a similar incident from reoccurring in the future.

1. **Nature of the incident.**

In September 2020, Timberline notified approximately 190 school districts that Timberline experienced a cybersecurity incident which resulted in the exposure of personal information maintained by educational institutions and processed by Timberline. Cedar Falls CSD was first notified of this incident by Timberline on September 2, 2020.

On March 5, 2020, Timberline noticed suspicious activity on its network impacting certain servers and systems. Timberline launched an investigation to determine the nature and scope of this activity. Working with outside computer forensics specialists, Timberline determined that an unknown actor accessed Timberline's network between February 12, 2020 and March 4, 2020, encrypted certain files, and also removed certain information from Timberline's network; however, the investigation was unable to determine which specific information was actually removed. Therefore, out of an abundance of caution, Timberline undertook a comprehensive and time-intensive review of all files that could have been impacted. This review was recently completed and determined that protected health information and/or personal information relating to your child was present in files that may have been compromised.

Based on the investigation, Timberline discovered that the following Personally Identifiable Information ("PII") was compromised: Individual's name in combination with their Medicaid

Identification Number, Driver License Number and State Identification Number. To date, Timberline is unaware of any actual or attempted misuse of personal information as a result of this incident.

2. **Number of Iowa residents affected.**

Cedar Falls CSD finished reviewing the list of affected individuals on October 14, 2020 and determined one thousand four hundred eighteen (1,418) Iowa residents were potentially affected. Incident notification letters addressed to those individuals were mailed on November 2, 2020 via First Class Mail. A sample copy of the Incident notification letter mailed to potentially affected residents of Iowa is included with this letter at **Exhibit A**.

3. **Steps taken.**

Upon learning of this incident, Timberline moved quickly to investigate and respond to the incident, assess the security of relevant Timberline systems, and identify potentially affected individuals. Timberline also reported this incident to law enforcement. Timberline is taking steps to enhance the security of its systems in addition to the robust security measures already in place including upgrading all servers and firewalls, resetting all user passwords and requiring frequent password rotations, and migrating school and student data to a cloud location.

Timberline is also offering complimentary credit monitoring and identity theft restoration services for twelve months to affected residents. Cedar Falls CSD takes the security, privacy, and confidentiality of its students' information very seriously and is encouraging its students to remain vigilant in response to this incident. Cedar Falls CSD is also encouraging its students to enroll in the complimentary credit monitoring services being provided by Timberline.

4. **Contact information.**

Cedar Falls CSD remains dedicated to protecting its students' sensitive personal information. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

Enclosure

EXHIBIT A

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

November 2, 2020

F9167-L31-0000009 T00001 P001 **********MIXED AADC 159
PARENT OR GUARDIAN OF
SAMPLE A SAMPLE - L31 CEDAR FALLS - MINOR
APT 123
123 ANY ST
ANYTOWN, US 12345-6789

Dear Parent or Guardian of Sample A Sample:

Notice of Data Event

Out of an abundance of caution, we are writing to inform you of a data security incident involving Timberline Billing Services, LLC ("Timberline"). Cedar Falls Community School District takes the security of your child's information very seriously, and we sincerely apologize for any inconvenience this incident may cause. While we are unaware of any actual misuse of your child's information, we are providing you with information about the incident, Timberline's response, and the steps you may take to better protect against possible misuse of your child's personal information, should you feel it necessary to do so.

Who is Timberline and Why Did They Have My Information?

Timberline provides Medicaid reimbursement billing services for covered IEP services to 190 school districts in Iowa, including Cedar Falls Community School District. In September 2020, Timberline notified Cedar Falls Community School District that Timberline experienced a cybersecurity incident which resulted in the exposure of personal information maintained by educational institutions and processed by Timberline. Cedar Falls Community School District was first notified of this incident by Timberline on September 2, 2020.

What Happened?

On March 5, 2020, Timberline noticed suspicious activity on its network impacting certain servers and systems. Timberline launched an investigation to determine the nature and scope of this activity. Working with outside computer forensics specialists, Timberline determined that an unknown actor accessed Timberline's network between February 12, 2020 and March 4, 2020, encrypted certain files, and also removed certain information from Timberline's network; however, the investigation was unable to determine which specific information was actually removed. Therefore, out of an abundance of caution, Timberline undertook a comprehensive and time-intensive review of all files that could have been impacted. This review was recently completed and determined that protected health information and/or personal information relating to your child was present in files that may have been compromised.

What Information Was Involved?

Based on the information we have received from Timberline, Timberline's investigation determined the following types of your child's information was involved: name and [Extra2 - Data Elements]. To date, Timberline is unaware of any actual or attempted misuse of personal information as a result of this incident.

What is Being Done in Response to this Incident?
The security, privacy, and confidentiality of your child's personal information are among our highest priorities. Upon learning of this incident, Timberline moved quickly to investigate and respond to the incident, assess the security of relevant Timberline systems, and identify potentially affected individuals. Timberline also reported this incident to law enforcement. Timberline is taking steps to enhance the security of its systems in addition to the robust security measures already in place including upgrading all servers and firewalls, resetting all user passwords and requiring frequent password rotations, and migrating school and student data to a cloud location.

While we are unaware of any misuse of your child's information as a result of this incident, Timberline is offering your child access to 12 months of minor identity monitoring through Experian at no cost to you. This product provides superior identity detection and resolution of identity theft. To activate this membership and start monitoring your minor's personal information please follow the steps below:

- Ensure that you **enroll by**: **January 31, 2021.** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/minorplus
- Provide your **activation code**: **ABCDEFGHI**
- Provide your minor's information when prompted

If you have questions about the product, need assistance with identity restoration for your minor or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (844) 439-7669 by **January 31, 2021.** Be prepared to provide engagement number **DB23497** as proof of eligibility for the identity restoration services by Experian.

Additional details regarding the 12-MONTH EXPERIAN IDENTITYWORKS Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks for your minor:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **Internet Surveillance**: Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: Receive the same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

If you believe there was fraudulent use of your minor's information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (844) 439-7669 If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to your minor for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

We encourage you to remain vigilant in response to this incident and encourage you to enroll in the complimentary credit monitoring services provided to you. Please refer to the attached addendum which includes additional information and steps you can take to further safeguard your child's personal information.

The protection of your child's information is among our highest priorities, and we sincerely regret any concern or inconvenience that this matter may cause your family. If you have additional questions or concerns, please call the toll-free dedicated assistance line at (844) 439-7669. This toll-free line is available Monday – Friday from 8:00 am to 10:00 pm CT, and Saturday – Sunday from 10:00 am to 7:00 pm CT.

Sincerely,

Dr. Andrew Pattee, Ed.D., *Superintendent*

Cedar Falls Community Schools

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 Maryland, Rhode Island, Illinois, New York and North Carolina: You can obtain information from the Maryland and North Carolina 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.com

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

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 District of Columbia: Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001 (202) 442-9828 https://oag.dc.gov/consumer-protection

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
www.freeze.equifax.com
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
PO Box 589
Claysburg, PA 16625-0589

November 2, 2020

F9167-L32-0000010 T00001 P001 **********MIXED AADC 159
SAMPLE A SAMPLE - L32 CEDAR FALLS - ADULT
APT 123
123 ANY ST
ANYTOWN, US 12345-6789

Dear Sample A Sample:

Notice of Data Event

Out of an abundance of caution, we are writing to inform you of a data security incident involving Timberline Billing Services, LLC ("Timberline"). Cedar Falls Community School District takes the security of your information very seriously, and we sincerely apologize for any inconvenience this incident may cause. While we are unaware of any actual misuse of your information, we are providing you with information about the incident, Timberline's response, and the steps you may take to better protect against possible misuse of your personal information, should you feel it necessary to do so.

Who is Timberline and Why Did They Have My Information?

Timberline provides Medicaid reimbursement billing services for covered IEP services to 190 school districts in Iowa, including Cedar Falls Community School District. In September 2020, Timberline notified Cedar Falls Community School District that Timberline experienced a cybersecurity incident which resulted in the exposure of personal information maintained by educational institutions and processed by Timberline. Cedar Falls Community School District was first notified of this incident by Timberline on September 2, 2020.

What Happened?

On March 5, 2020, Timberline noticed suspicious activity on its network impacting certain servers and systems. Timberline launched an investigation to determine the nature and scope of this activity. Working with outside computer forensics specialists, Timberline determined that an unknown actor accessed Timberline's network between February 12, 2020 and March 4, 2020, encrypted certain files, and also removed certain information from Timberline's network; however, the investigation was unable to determine which specific information was actually removed. Therefore, out of an abundance of caution, Timberline undertook a comprehensive and time-intensive review of all files that could have been impacted. This review was recently completed and determined that protected health information and/or personal information relating to you was present in files that may have been compromised.

What Information Was Involved?

Based on the information we have received from Timberline, Timberline's investigation determined the following types of your information was involved: name and [Extra2 - Data Elements]. To date, Timberline is unaware of any actual or attempted misuse of personal information as a result of this incident.

What is Being Done in Response to this Incident?
The security, privacy, and confidentiality of your personal information are among our highest priorities. Upon learning of this incident, Timberline moved quickly to investigate and respond to the incident, assess the security of relevant Timberline systems, and identify potentially affected individuals. Timberline also reported this incident to law enforcement. Timberline is taking steps to enhance the security of its systems in addition to the robust security measures already in place including upgrading all servers and firewalls, resetting all user passwords and requiring frequent password rotations, and migrating school and student data to a cloud location.

While we are unaware of any misuse of your information as a result of this incident, Timberline is offering you access to 12 months of identity credit monitoring through Experian at no cost to you. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **January 31, 2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (844) 439-7669 by **January 31, 2021.** Be prepared to provide engagement number **DB23496** as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your 12-month Experian IdentityWorks Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only. *
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

** Offline members will be eligible to call for additional reports quarterly after enrolling.*

*** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (844) 439-7669. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

We encourage you to remain vigilant in response to this incident and encourage you to enroll in the complimentary credit monitoring services provided to you. Please refer to the attached addendum which includes additional information and steps you can take to further safeguard your personal information.

The protection of your information is among our highest priorities, and we sincerely regret any concern or inconvenience that this matter may cause you. If you have additional questions or concerns, please call the toll-free dedicated assistance line at (844) 439-7669. This toll-free line is available Monday – Friday from 8 am to 10 pm CT, and Saturday - Sunday from 10 am to 7 pm CT.

Sincerely,

Dr. Andrew Pattee, Ed.D., *Superintendent*

Cedar Falls Community Schools

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 Maryland, Rhode Island, Illinois, New York and North Carolina: You can obtain information from the Maryland and North Carolina 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.com

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

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 District of Columbia: Office of Consumer Protection, 400 6th Street, NW, Washington, DC 20001 (202) 442-9828 https://oag.dc.gov/consumer-protection

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
www.freeze.equifax.com
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 than 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 twenty-four (24) 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 two years 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.