Michael Best & Friedrich LLP
Attorneys at Law
Elizabeth A. Rogers, CIPP/US
T 512.640.3164
E earogers@michaelbest.com

May 5, 2021

VIA FEDEX

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

RE: Data Breach Notification

Attorney General Gordon J. MacDonald:

Pursuant to N.H. Rev. Stat. §359-C:19, et seq., Ultratec, Inc., 450 Science Dr, Madison, WI 53711 ("Ultratec" or the "Company"), through its attorneys Michael Best & Friedrich, LLP, 620 Congress Avenue, Suite 200, Austin, TX 78701 ("MBF"), is writing to provide this notice of a security breach that affected its systems. Ultratec develops text telecommunications services and equipment that enable people who are deaf or hard of hearing to communicate over the telephone. Kevin Colwell, Vice President Engineering, kevin.colwell@ultratec.com, (608) 238-5400, is Ultratec's contact, and Elizabeth A. Rogers, Partner, earogers@michaelbest.com, (512) 640-3164, from MBF is Ultratec's legal counsel, assisting with the management of this incident.

Ultratec believes that five (5) New Hampshire residents were impacted by this breach. Ultratec is providing these individuals with 12 months of free credit monitoring services through Equifax.

On or about November 4, 2020, Ultratec, experienced a security incident as a result of malware that was likely installed on its systems on or about October 9, 2020. The malware allowed a threat actor to encrypt and acquire certain Company information. Additionally, the malware destroyed four different servers containing hundreds of thousands of documents. Ultratec responded to the incident immediately, by disconnecting endpoints and external connections from the network and remediating the vulnerability.

Since then, Ultratec has been carefully and diligently responding to the incident by promptly engaging counsel, and multiple vendors, including an expert IT Forensics provider. Ultratec's forensics provider was hired to not only determine the cause of the security incident and determine whether there was ongoing infection, but to also engage in a series of negotiations with the threat actor. Ultimately, the negotiations resulted in an agreement by the threat actors to delete the data that it had acquired. There is no evidence that the stolen information was misused or not shared with any person other than the threat actors.

Meanwhile, the damage to the servers delayed Ultratec's ability to review impacted documents on those servers. Ultratec ultimately had to rebuild its affected systems and take additional precautions to upgrade to an Office 365 environment, install an industry leading advanced Endpoint Threat Detection and Mitigation utility, and rebuild remote access to new standards. This undertaking required Ultratec to engage and consult with various third-party vendors with expertise in the relevant systems and security measures employed in its rebuild and remediation.

After Ultratec repaired its systems, Ultratec engaged a third-party e-discovery firm to review the data that was on the affected servers. Because of, among other things, the large volume of documents identified for review and the number of documents that required manual review, that review was time-intensive and required that the e-discovery vendor engaging eighty (80) or more individuals to review the documents. Because of the necessity to rebuild systems and the time-consuming nature of the review, Ultratec was not able to formulate a comprehensive list of affected individuals until end of April 22, 2021.

The personal information that may have been accessed included: name, address, telephone number, date of birth, social security number, government or state issued ID, passport number, military ID, driver's license number, student ID, financial account information, username and password, medical information, and health insurance member or group number.

As set forth above, Ultratec took several measures to respond to the incident. Ultratec further notified and consulted with law enforcement with respect to its response, but the law enforcement investigation did not delay notification to you.

Attached is a copy of the notification letter that Ultratec will place in the U.S. Mail Wednesday, May 5, 2021 to the affected individuals. There was no delay in providing individual notification as a result of law enforcement investigation. Please let us know if you have any questions or would like to discuss further.

Sincerely,

MICHAEL BEST & FRIEDRICH LLP

Elizabeth A. Rogers

Enclosure

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>>

Notice of Data Breach

Dear <<Name 1>>:

We are writing to inform you about a data security incident that affected the systems of Ultratec, Inc. and its affiliated entities, including, but not limited to, CapTel, Inc., Captel Service Specialists, LLC, and Weitbrecht Communications, Inc. (collectively, "Company" or "Ultratec") that may have involved your personal information. Ultratec takes the security of your information very seriously. We are therefore contacting you to explain the incident and provide you with steps you can take to protect yourself.

What Happened
On or about November 4, 2020, Ultratec experienced a security incident that damaged some of its systems and allowed an unauthorized third party to acquire certain Company information. The security incident was likely the result of malware installed on Ultratec's system on or about October 9, 2020. Ultratec responded immediately, by disconnecting the network from external connections and remediating the vulnerability. Since then, Ultratec has been engaging third party experts to rebuild its affected systems and upgrade software in order to carefully determine what information was impacted.

What Information Was Involved
The personal information that the threat actors acquired may include your name, address, telephone number, date of birth, social security number, government or state issued ID, passport number, military ID, driver's license number, student ID, financial account information, username and password, medical information, and health insurance member or group number. While this information may have been accessed, we do not have any evidence that it was either misused or disclosed to anyone other than the threat actors themselves.

What We Are Doing
We have engaged third party cybersecurity experts to respond to and investigate this incident, as well as restore and secure our systems to determine what information was impacted. In addition, we have enhanced the security of our systems and installed industry leading advanced endpoint threat detection and mitigation tools. We further notified and consulted with law enforcement with respect to our response, but the law enforcement investigation did not delay notification to you.

We have also notified our credit card payment processor of the incident so that the card brands are also notified and are aware of the incident with respect to your information.

What You Can Do
In addition, we are providing you with the enclosed information about Identity Theft Protection. To help protect you, we have retained Equifax, a specialist in identity theft prevention to provide you with 12 months of credit monitoring services, free of charge. To enroll in Equifax Credit Watch Gold services, please see the attached enrollment instructions. If you see anything that looks suspicious, call the credit agency immediately. You should also regularly review your credit or debit card account statements to determine if there are any discrepancies or unusual activity listed. If you see something you do not recognize, immediately notify your financial institution.

For More Information
We take the security and privacy of your information very seriously and apologize for any inconvenience this incident may have caused. For information related to this matter, please call our toll-free dedicated assistance line at 855-654-0887, Monday – Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, except holidays. Should you have any further questions or concerns, please contact privacyreports@ultratec.com.

Sincerely,

Jayne Turner
Vice President

Information about Identity Theft Protection

Review Accounts and Credit Reports: It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies. To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:
Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: 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.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For residents of Rhode Island: You may also obtain information about preventing and avoiding identity theft from Rhode Island Attorney General's Office: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, http://www.riag.ri.gov.

For residents of District of Columbia: You may also obtain information about preventing and avoiding identity theft from District of Columbia Attorney General's Office: District of Columbia Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001, 202-727-3400, https://oag.dc.gov/

For residents of New York: You may also obtain information about preventing and avoiding identity theft from: New York Department of State Division of Consumer Protection: http://www.dos.ny.gov/consumerprotection and NYS Attorney General at: http://www.ag.ny.gov/home.html

Security Freezes and Fraud Alerts:

You have a right to place a security freeze on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. There is no fee for a security freeze. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

Additional Information for Massachusetts Residents: Massachusetts law gives you the right to place a security freeze on your consumer reports at no charge. By law, you have a right to obtain a police report relating to this incident, and if you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number, date of birth (month, day and year); current address and previous addresses for the past five (5) years; and an incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

Additional Information for New Mexico Residents: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. Here is a summary of your major rights under the FCRA:

- You have the right to be told if information in your file has been used against you;
- You have the right to receive a copy of your credit report and the right to ask for a credit score;
- You have the right to dispute incomplete or inaccurate information;
- You have the right to dispute inaccurate, incomplete, or unverifiable information;
- You have the right to have outdated negative information removed from your credit file;
- You have the right to limit access to your credit file;
- You have the right to limit "prescreened" offers of credit and insurance you get based on information in your credit report;
- You have the right to seek damages from violators; and
- You have the right to place a "security freeze" on your credit report.

New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and may need to provide all of the following:

(1) the unique personal identification number, password or similar device provided by the consumer reporting agency;

(2) proper identification to verify your identity; and

(3) information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of pre-screening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

For more information, including information about additional rights, you can visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf,https://www.consumerfinance.gov/learnmore/, or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

EQUIFAX P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 www.equifax.com	**EXPERIAN** Consumer Fraud Assistance P.O. Box 9554 Allen, TX 75013 888-397-3742 www.experian.com	**TRANSUNION** P.O. Box 2000 Chester, PA 19016-2000 Phone: 800-909-8872 www.transunion.com

EQUIFAX®

Enter your Activation Code: <<ACTIVATION CODE>>
Enrollment Deadline: <<Enrollment Deadline>>

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 <<ACTIVATION CODE>> 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.*

To sign up for US Mail delivery, dial 1-855-833-9162 for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.

1. **Activation Code:** You will be asked to enter your enrollment code as provided at the top of this letter.
2. **Customer Information:** You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.
3. **Permissible Purpose**: You will be asked to provide Equifax with your permission to access your Equifax credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment.
4. **Order Confirmation**: Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.