22212

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

Via First Class Mail

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

Central Texas Medical Specialists PLLC dba Austin Cancer Centers ("Austin Cancer Centers") provides this notice of data breach as part of its commitment to patient privacy. We deeply regret that his happened, and aim to do everything possible to help you understand and navigate steps to keep yourself protected from any risk.

What Happened

Austin Cancer Centers experienced a security breach to their technology and information systems involving unauthorized access and malware. The breach was discovered on August 4, 2021 and the systems were immediately shut down, and law enforcement contacted. Forensic teams uncovered that the breach began on July 21, 2021, and that the unauthorized user had used sophisticated technology to remain invisible in the system. Due to security reasons, it took 14 days to identify, uncover and release the information. It also required the technology systems within the Austin Cancer Centers to remain shut down. During this time, we worked to manually maintain operations as best as possible, and to continue to support our patients with top notch treatment. We hope this did not create any inconveniences in your care.

What Information Was Involved

Austin Cancer Centers determined that the following protected health information may have been affected by the incident: First name, last name, address, date of birth, social security number, diagnosis, diagnosis code, current procedural terminology codes, insurance carrier name, condition, lab results, medication, or other related information. A very limited number of patients personally wrote down their credit card information and submitted via mail to our offices. These patients may have had their credit card information affected.

What We Are Doing

Austin Cancer Centers aggressively took steps to mitigate harm to your data and end the breach. A nationally recognized forensics company was retained to investigate the incident, monitor our systems, and provide assistance. We have a dedicated team of computer experts working daily to fully restore and protect your data. The Federal Bureau of Investigations and Austin Police Department have been notified and a police report was made. If you would like a free copy of the police report filed with the Austin Policy Department, please call or write using the toll-free number and address found at the end of this letter. Our entire staff have undergone retraining related to this incident, and we have implemented additional technical safeguards and procedures to prevent this kind of incident from happening again. We continue to evaluate the situation and implement appropriate safeguards as needed.

What You Can Do

We are deeply sorry for any concern this incident may have caused you. In response to this incident, we have arranged for you to enroll for two years, free-of-charge, in an online credit monitoring service called Equifax Credit Watch™ Gold. Key features of this complimentary service include credit monitoring with email notifications, automatic fraud alerts, and up to $1,000,000 of identity theft services for certain out of pocket expenses resulting from identity theft. Please carefully review the enclosed enrollment form which has your Activation Code and Enrollment Deadline.

Whether or not you enroll in credit monitoring, we recommend that you place a "Fraud Alert" on your credit file. Fraud Alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. Call only one of the following three nationwide credit reporting companies to place your Fraud Alert: TransUnion, Equifax, or Experian. As soon as the credit reporting company confirms your Fraud Alert, they will also forward your alert request to the other two nationwide credit reporting companies so you do not need to contact each of them separately. The contact information for the three nationwide credit reporting companies is:

Equifax	**Experian**	**TransUnion**
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
(800) 685-1111	(888) 397-3742	(800) 680-7289

Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly. It is generally recommended that individuals can help further secure their online accounts by regularly changing their user names and passwords and security questions and answers.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You can also report suspected incidents of identity theft to the attorney general of your state. You also should file a complaint with the Federal Trade Commission (FTC) at www.identitytheft.gov or at 1-877-ID-THEFT (1-877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations. Also visit the FTC's website at www.ftc.gov/idtheft to review their free identity theft resources such as their comprehensive step-by-step guide "*Identity Theft - A Recovery Plan*".

You can request a "Security Freeze" on your credit file by sending a request in writing, by mail, to each of the three nationwide credit reporting companies. When a Security Freeze is added to your credit report, all third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. The Security Freeze may delay, interfere with or prohibit the timely approval of any subsequent request or application you make that involves access to your credit report. This may include, but is not limited to, new loans, credit, mortgages, insurance, rental housing, employment, investments, licenses, cellular phone service, utility service, digital signature service, Internet credit card transactions and extension of credit at point of sale. There may be a fee for placing, temporarily lifting, or removing a Security Freeze with each of the nationwide consumer reporting companies, although that fee is waived if you send the credit reporting company proof of eligibility by mailing a copy of a valid identity theft report, or other valid report from a law enforcement agency to show you are a victim of identity theft and are eligible for free Security Freeze services. Please contact Austin Cancer Centers if you are charged a fee for placing a credit freeze, and we will work with you to resolve the charge.

For More Information

We understand you may have questions about this incident or need assistance enrolling in credit monitoring services. Please use the following toll-free number if you would like to speak with a representative: 800-708-1979. The call center is available Monday through Friday, 8:00 a.m. to 8:00 p.m., Central Time, except holidays. This toll-free number will be valid for the next 90-days. You can also contact Austin Cancer Centers at the following address: Austin Cancer Centers, Attn: Privacy Officer, 9715 Burnet Rd building 7 suite 200, Austin, TX 78758.

Unfortunately, no organization is immune from cyber criminals and attacks today. Please be assured that Austin Cancer Centers is giving this incident its full attention and is dedicated to the matter. We apologize for any inconvenience this incident has caused you, and we are committed to working with you to answer all of your questions. And for any questions related to your treatment or care, please continue to contact our offices.

Sincerely,

Austin Cancer Centers

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.*

Additional Information

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General for the District of Columbia (https://oag.dc.gov/), 400 6 Street, NW, Washington, D.C. 20001, Telephone (202) 727-3400.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: All US residents should remain vigilant by reviewing account statements and monitoring their credit reports. Additional resources may be obtained at the Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.