

Additional 17938

[EXTRA3]
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

December 7, 2020



G0181-L01-0000001 T00001 P001 *****ALL FOR AADC 159
SAMPLE A SAMPLE - ADULT - FA
123 ANY STREET
ANYTOWN, US 12345-6789



Re: Notice of Data Breach

Dear Sample A Sample:

[EXTRA3] d/b/a [EXTRA4] (hereinafter “[EXTRA4]” or “Practice”) is writing to notify you of an incident that may affect the security of some of your personal information. The Practice is advising you of its investigation and the steps it has taken in response to the incident. The Practice is also providing you with steps you can take to help protect your personal information should you feel it is appropriate to do so.

What Happened? On October 11, 2020, [EXTRA4] became aware of suspicious activity in its environment and immediately initiated an investigation into the incident. As part of the investigation, which is being conducted with the assistance of third-party forensic specialists, it was determined that unauthorized individuals accessed certain files on the Practice’s network between September 18, 2020 and October 13, 2020. Therefore, with the assistance of our third-party specialists, we conducted a review of the files at risk to identify any individuals whose sensitive information could be impacted. Through the review, [EXTRA4] determined that information related to you was contained in the files. Although there is no specific evidence that your information was actually viewed by the unauthorized individuals, and we have seen no evidence to date that any data has been used for malicious purposes, we are providing this notice to you in an abundance of caution.

What Information Was Involved? The information that was potentially subject to unauthorized access includes your name, address, dental diagnosis and treatment information, patient account number, billing information, dentist’s name, bank account number, and health insurance information.

What We Are Doing. The Practice takes the security of personal information in our care very seriously. You are being notified because your personal information may have been subject to unauthorized access. This does not mean you are a victim of identity theft. As part of our ongoing commitment to the protection of information in our care, we worked with third-party specialists to reaffirm the security of our systems and to enhance the existing measures we have in place. We have already taken and will continue to take steps to help reduce the likelihood of a similar situation in the future, including enhanced employee training, mandatory password changes, and systems upgrades. We also notified the United States Department of Health and Human Services and state regulators, as required.

What You Can Do. As a best practice, you should always review your account statements for suspicious or unauthorized activity and report any instances of fraud to law enforcement. We also encourage you to review the enclosed *Steps You Can Take to Protect Against Identity Theft and Fraud*. There you will find general information on what you can do to help protect your personal information.

0000001



G0181-L01

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance, please call 877-672-4690 (toll free) Monday through Friday from 9:00 am to 11:00 pm or Saturday and Sunday from 11:00 am to 8:00 pm Eastern Time. The Engagement Number for this matter is DB24136.

Sincerely,

[EXTRA4]

Steps You Can Take to Help Protect Against Identity Theft and Fraud

Monitor Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the 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. 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. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872

www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111

www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services



Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

For 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 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. We encourage you to 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.

For 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/>.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Rhode Island residents, the Attorney General may be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov.

For Washington, D.C. residents, the Office of Attorney General for the District of Columbia can be reached at 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; 1-202-442-9828; <https://oag.dc.gov>.