


Bassett Family Practice

HIPAA BREACH NOTIFICATION

WHAT HAPPENED AND INFORMATION INVOLVED

On August 14, 2017, it was discovered that an employee's laptop had been stolen out of his/her car. We believe the theft occurred between the evening of August 12, 2017 and the discovery that the laptop was missing, on the morning of August 14, 2017. The theft was immediately reported to law enforcement officials, and we continue to work with law enforcement in an effort to recover the device. At this point in time, we have no reason to think that the information was the target of the theft or that the information has been accessed or used by an unauthorized individual. We are also monitoring any activity associated with the laptop, and if the laptop is used to access the internet we will wipe the contents of the laptop completely and permanently.

As a result of our investigation into the theft of the laptop computer, we have learned that a limited amount of your personal information, including (full name, date of birth, account number, identity of your provider, and/or details about your visit with the practice) may have been located on the stolen laptop. There is no indication at this time that your social security number or financial account information (bank account numbers, credit card numbers) were located on the stolen laptop.

WHAT WE ARE DOING IN RESPONSE

We sincerely apologize for any inconvenience or concern this incident may cause you. We are currently upgrading our IT security policies, procedures and related equipment to prevent future information from being stored on a laptop in an unencrypted manner. Please understand we value our relationship with you and take the security of your personal information very seriously. We have taken immediate steps and we will continue to evaluate our technology, policies and procedures in our efforts to prevent another occurrence such as this from happening in the future.

WHAT YOU CAN DO IN RESPONSE

Review of Accounts and Credit Reports-As part of your ongoing vigilance regarding the protection of your identify and financial security, we urge you to regularly review statements from you accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You can obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Request Form (available at www.annualcreditreport.com) to: Annual credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the end of this guide.

Remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the relevant government institution and 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 protection against identify theft: Federal Trade Commission, Consumer

Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft. There may be similar resources available at the state level, and you may contact your state department of revenue directly for more information.

Residents of Virginia may also obtain information about preventing and avoiding identity theft from the Virginia Attorney General's Office: by mailing the Office of the Attorney General, Victim Notification Program, 202 North Ninth Street, Richmond, VA 23219 or by visiting the website <https://www.oag.state.va.us/programs-initiatives/identity-theft>.

Fraud Alerts-There are also two types of fraud alerts that you can place on your credit report to put creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may request an initial fraud alert if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies listed below or visit the website <https://www.consumer.ftc.gov/articles/0275-place-fraud-alert>.

Credit Freezes- You may have the right to put a credit freeze, also known as a security freeze, on your credit file so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

Contact information for the three National credit agencies

TransUnion

1-800-680-7289

www.transunion.com

Experian

1-888-397-3742

www.experian.com

Equifax

1-800-525-6285

www.experian.com

FOR MORE INFORMATION

If you have any questions or for further information and assistance, please contact our toll free assistance line at 1-888-746-7175.

We are committed to keeping your personal information safe. Again, we sincerely apologize for any concern or inconvenience this matter may cause you.