



Richard W. Goldberg
550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Richard.Goldberg@lewisbrisbois.com
Direct: 215.977.4060

July 7, 2022

VIA EMAIL

Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
ldtheft@oag.state.md.us

Re: Notification of Data Security Incident

Dear Attorney General Frosh:

We represent Family Practice Center PC ("Family Practice"), which operates full service medical facilities headquartered in Middleburg, PA, in connection with a data security incident described in greater detail below. Family Practice takes the protection of all sensitive information within its possession very seriously and is taking steps to prevent similar incidents from occurring in the future.

1. Nature of the security incident.

On October 11, 2021, someone attempted to interfere with the operations of Family Practice's computer system. That attempt largely failed and Family Practice was still able to treat patients and provide service to the community. Family Practice immediately launched an investigation to determine what happened and what information may have been accessed by an unauthorized person during the incident. On May 21, 2022, the investigation revealed that some of the files accessed contained personal information of patients. While at this time we have no evidence that any information has been misused, out of an abundance of caution, we are providing credit monitoring and identity theft protection to patients whose Social Security information may have been involved in the incident. The potentially affected information includes names, addresses, Social Security numbers, medical insurance information and health and treatment information. On June 30, 2022, Family Practice determined current address information for the affected individuals in order to effectuate written notification of the incident. This investigation identified seventy-eight (78) Maryland residents within the affected population. Notification letters were mailed on July 7, 2022.

2. Number of Maryland residents affected.

Family Practice issued notification letters to the seventy-eight (78) Maryland residents regarding this data security incident via first-class U.S. mail on July 7, 2022. A sample copy of the notification letter is attached hereto.

3. Steps taken relating to the incident.

Family Practice has taken steps in response to this incident to prevent similar incidents from occurring in the future. Those steps have included working with leading cybersecurity experts to advise regarding the security of its network and its password complexity requirements. Family Practice is also offering the potentially affected individuals whose Social Security numbers were impacted credit and identity monitoring at no cost, to ensure their information is protected.

4. Contact information.

Family Practice remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at (215) 977-4060 or via email at Richard.Goldberg@lewisbrisbois.com.

Regards,

/s/ Richard W. Goldberg

Richard W. Goldberg of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure(s): Consumer Notification Letters



P.O Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zipcode>>

July 7, 2022

Re: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

Family Practice Center PC ("Family Practice") is writing to inform you about an incident that may have involved your personal information. We take the privacy and security of our patient information very seriously. Therefore, we are writing to inform you about the incident.

What Happened? On October 11, 2021, we discovered an attempt to interfere with our computer system. That attempt largely failed and we were able to continue serving our patient community. We immediately launched an investigation to determine what happened and what information may have been accessed by an unauthorized person during the incident. That investigation revealed, on May 21, 2022, whose information may have been involved in the incident. We have no evidence that any information has been misused.

What Information Was Involved? The files that may have been accessed contained your name, <<Variable 1>>. Patient medical records were not involved in the incident.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. We also reported the incident to law enforcement and will continue to cooperate with their investigation. We have also made adjustments to help prevent the reoccurrence of a similar incident.

If you have questions or need assistance, please call 1-833-909-4308.

What You Can Do: Please review the enclosed information describing additional steps you can take to help safeguard your information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For More Information: If you have questions or need assistance, please call 1-833-909-4308 Monday through Friday from 9 a.m. to 9 p.m. Eastern Time.

*Family Practice Center, PC
7 Dock Hill Road
Middleburg, PA 17842
(570) 743-1703*

Protecting your information is important to us. Please know that we take this incident very seriously, and we regret any concern this may cause you.

Sincerely,

Family Practice Center Board of Directors

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.



P.O Box 989728
West Sacramento, CA 95798-9728

To the Family Member of:

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zipcode>>

July 7, 2022

Re: Notice of Data Security Incident

Dear Family Member of <<First Name>> <<Last Name>>,

Family Practice Center PC ("Family Practice") is writing to inform you about an incident that may have involved your family member's personal information. We take the privacy and security of our patient information very seriously. Therefore, we are writing to inform you about the incident.

What Happened? On October 11, 2021, we discovered an attempt to interfere with our computer system. That attempt largely failed and we were able to continue serving our patient community. We immediately launched an investigation to determine what happened and what information may have been accessed by an unauthorized person during the incident. That investigation revealed, on May 21, 2022, whose information may have been involved in the incident. We have no evidence that any information has been misused.

What Information Was Involved? The files that may have been accessed contained your family member's name, <<Variable 1>>. Patient medical records were not involved in the incident.

What Are We Doing? As soon as we discovered the incident, we took the steps described above. We also reported the incident to law enforcement and will continue to cooperate with their investigation. We have also made adjustments to help prevent the reoccurrence of a similar incident.

If you have questions or need assistance, please call 1-833-909-4308.

What You Can Do: Please review the enclosed information describing additional steps you can take to help safeguard your family member's information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your family member's credit file.

For More Information: If you have questions or need assistance, please call 1-833-909-4308 Monday through Friday from 9 am - 9 pm Eastern Time.

*Family Practice Center, PC
7 Dock Hill Road
Middleburg, PA 17842
(570) 743-1703*

Protecting your family member's information is important to us. Please know that we take this incident very seriously, and we regret any concern this may cause you.

Sincerely,

Family Practice Center Board of Directors

Steps You Can Take To Protect Your Family Member's Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your family member's account statements and credit reports closely. If you detect any suspicious activity on an account related to your family member, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: In order to obtain a copy of your family member's credit report, you will need to provide proof that you are authorized to act on their behalf. This often occurs when the credit bureau is initially informed of their passing with a copy of their death certificate, and a copy of the legal document authorizing you to act on their behalf. You may then obtain a free copy of your family member's credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You should inform the credit reporting agencies that your family member is deceased, and you can do so with a copy of their death certificate and a copy of the legal document authorizing you to act on their behalf. You may then inform the credit reporting agencies of fraudulent activity that may involve your family member's identity. You may also want to consider placing a fraud alert on your own credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your family member's credit file for up to one year at no cost. This will prevent new credit from being opened in your family member's name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your family member's credit report without your consent. You must separately place a security freeze on your family member's credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies your family member including their full name, Social Security Number, date of birth, current and previous addresses, and copy of their state-issued identification card.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and
Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center

Raleigh, NC 27699

ncdoj.gov

1-877-566-7226

Rhode Island Attorney General

150 South Main Street

Providence, RI 02903

<http://www.riag.ri.gov>

1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW

Washington, DC 20001

oag.dc.gov

1-202-727-3400

Consumers have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in their file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and consumer rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>