

21768



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Dear<<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

At Orlando Family Physicians (OFP), we understand that the confidentiality and security of your personal information is very important, and we are committed to protecting it. We are sending you this notice to let you know that OFP was the victim of a recent phishing email incident that potentially resulted in unauthorized access to personal information we maintain about you. *At this time, we are not aware of any misuse of your personal information.*

WHAT HAPPENED?

On April 15, 2021, an unauthorized person accessed the email account of an OFP employee by obtaining the employee's user ID and password through a phishing email. We immediately took steps to contain the incident and began an investigation to determine its scope. We retained a leading cybersecurity forensics firm to assist with our investigation. As part of the investigation, we identified three additional employee email accounts that the unauthorized person accessed and began an extensive review of the affected email accounts to determine whether they contained personal information. We terminated the unauthorized access to each of the four affected employee email accounts within 24 hours of the initial unauthorized access to the account.

On May 21, 2021, OFP discovered that there may have been unauthorized access to personal information contained in the four email accounts. On July 9, 2021, OFP identified the OFP patients, prospective patients, employees and other individuals whose personal information was included in the affected email accounts. However, the available forensic evidence suggests that the unauthorized person's purpose was to attempt to commit financial fraud against OFP and not to obtain your personal information. Nonetheless, we are notifying you and other affected individuals because of the possibility that the unauthorized person had access to your personal information.

WHAT INFORMATION WAS INVOLVED?

The information contained in the affected OFP employees' email accounts included the following types of information about the affected individuals, but may not have included all of the types of information about you: name; contact information; passport number; date of birth; health information, including diagnoses and prescriptions; medical record number; patient account number; legacy Medicare beneficiary identification number which includes Social Security number; and other health insurance information.

WHAT WE ARE DOING

We have enhanced our data security measures to prevent the occurrence of a similar event in the future. We are also providing supplemental training to our employees on the importance of email security.

As noted above, we have no reason to believe that your information has been, or will be, misused because of this incident. Nonetheless, as a precautionary measure, we would like to offer you two years of free identity monitoring services from Kroll. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Please review the sheet enclosed with this letter for information about activating Kroll's identity monitoring services.

WHAT YOU CAN DO

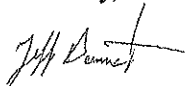
In addition to enrolling in the identity monitoring services from Kroll, we encourage you to follow the recommendations below:

- Read account statements from your health care providers, explanations of benefits (EOBs) from your health plan and other documents related to medical services to make sure they do not include services you did not receive.
- Be attentive to documents related to medical services that you usually receive and that suddenly do not arrive, as you usually receive them.
- All mail related to medical or financial information should be destroyed and preferably shredded before you throw it away.
- Be careful when offering personal information over the phone, mail or internet, and unless you are sure of the person with whom you are dealing, offer as little information as possible.
- Review the "General Information About Identity Theft Protection" materials that are included with this letter. You should always remain vigilant for threats of fraud and identity theft by regularly reviewing your account statements and credit reports.

FOR MORE INFORMATION

We regret this incident and apologize for any inconvenience it may cause you. If you have any questions or concerns, please contact us toll-free by calling 1-855-545-2005 Monday through Friday between 9:00 am and 6:30 pm Eastern Time, excluding major U.S. holidays.

Sincerely,



Jeff Bennett
President



ACTIVATE YOUR IDENTITY MONITORING SERVICES

Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

*You have until **October 27, 2021** to activate your identity monitoring services.*

Membership Number: <<Membership Number s_n>>

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Credit Reports. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You may contact the nationwide credit reporting agencies at:

Equifax
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
www.experian.com
(888) 397-3742

TransUnion
P.O. Box 2000
Chester, PA 19016
www.transunion.com
(800) 680-7289

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Place a Security Freeze on your Credit Report. You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed at above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. You can place a freeze and lift a security freeze on your credit report free of charge.

You may contact the Federal Trade Commission (FTC) and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the FTC and/or your state's attorney general office about for information on how to prevent or avoid identity theft. You can contact the FTC at: **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

If you are a **Massachusetts resident**, you have the right to obtain a police report if you are the victim of identity theft.



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

At Orlando Family Physicians (OFP), we understand that the confidentiality and security of your personal information is very important, and we are committed to protecting it. We are sending you this notice to let you know that OFP was the victim of a recent phishing email incident that potentially resulted in unauthorized access to personal information we maintain about you. *At this time, we are not aware of any misuse of your personal information.*

WHAT HAPPENED?

On April 15, 2021, an unauthorized person accessed the email account of an OFP employee by obtaining the employee's user ID and password through a phishing email. We immediately took steps to contain the incident and began an investigation to determine its scope. We retained a leading cybersecurity forensics firm to assist with our investigation. As part of the investigation, we identified three additional employee email accounts that the unauthorized person accessed and began an extensive review of the affected email accounts to determine whether they contained personal information. We terminated the unauthorized access to each of the four affected employee email accounts within 24 hours of the initial unauthorized access to the account.

On May 21, 2021, OFP discovered that there may have been unauthorized access to personal information contained in the four email accounts. On July 9, 2021, OFP identified the OFP patients, prospective patients, employees and other individuals whose personal information was included in the affected email accounts. However, the available forensic evidence suggests that the unauthorized person's purpose was to attempt to commit financial fraud against OFP and not to obtain your personal information. Nonetheless, we are notifying you and other affected individuals because of the possibility that the unauthorized person had access to your personal information.

WHAT INFORMATION WAS INVOLVED?

The information contained in the affected OFP employees' email accounts included the following types of information about the affected individuals, but may not have included all of the types of information about you: name; contact information; date of birth; health information, including diagnoses and prescriptions; medical record number; patient account number; and health insurance information, including subscriber identification number and claim number.

WHAT WE ARE DOING

We have enhanced our data security measures to prevent the occurrence of a similar event in the future. We are also providing supplemental training to our employees on the importance of email security.

WHAT YOU CAN DO

While we have no reason to believe that your information has been, or will be, misused because of this incident, we encourage you to follow the recommendations below:

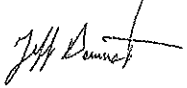
- Read account statements from your health care providers, explanations of benefits (EOBs) from your health plan and other documents related to medical services to make sure they do not include services you did not receive.
- Be attentive to documents related to medical services that you usually receive and that suddenly do not arrive, as you usually receive them.

- All mail related to medical or financial information should be destroyed and preferably shredded before you throw it away.
- Be careful when offering personal information over the phone, mail or internet, and unless you are sure of the person with whom you are dealing, offer as little information as possible.
- Review the "General Information About Identity Theft Protection" materials that are included with this letter. You should always remain vigilant for threats of fraud and identity theft by regularly reviewing your account statements and credit reports.

FOR MORE INFORMATION

We regret this incident and apologize for any inconvenience it may cause you. If you have any questions or concerns, please contact us toll-free by calling 1-855-545-2005 Monday through Friday between 9:00 am and 6:30 pm Eastern Time, excluding major U.S. holidays.

Sincerely,



Jeff Bennett
President

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Credit Reports. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You may contact the nationwide credit reporting agencies at:

Equifax
P.O. Box 105788
Atlanta, GA 30348
www.equifax.com
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
www.experian.com
(888) 397-3742

TransUnion
P.O. Box 2000
Chester, PA 19016
www.transunion.com
(800) 680-7289

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Place a Security Freeze on your Credit Report. You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed at above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. You can place a freeze and lift a security freeze on your credit report free of charge.

You may contact the Federal Trade Commission (FTC) and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the FTC and/or your state's attorney general office about for information on how to prevent or avoid identity theft. You can contact the FTC at: **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

- If you are an **Iowa resident**, state law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590.
- If you are a **Maryland resident**, you may obtain additional information about preventing identity theft from the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us.
- If you are a **Massachusetts resident**, you have the right to obtain a police report if you are the victim of identity theft.
- If you are a **New Mexico resident**, you have certain rights pursuant to the federal Fair Credit Reporting Act (FCRA). For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.
- If you are a **North Carolina resident**, you may obtain additional information about preventing identity theft from the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, 1-877-566-7226.
- If you are an **Oregon resident**, state law advises you to report any suspected identity theft to law enforcement or to the FTC.
- If you are a **Rhode Island resident**, you can contact the Office of the Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov/>, (401) 274-4400.