RECEIVED
NOV 28 2022
CONSUMER PROTECTION

JacksonLewis

Jackson Lewis P.C.
Park Center Plaza I, Suite 400
6100 Oak Tree Blvd.
Cleveland, OH 44131
(216) 750-0404 Main
(216) 750-0826 Fax
www.jacksonlewis.com

Jackson Biesecker
Direct: (216) 750-4303
Jackson.Biesecker@jacksonlewis.com

VIA FIRST-CLASS MAIL
Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Data Incident Notification[1]

November 21, 2022

Dear Sir or Madam:

We are writing on behalf of our client, Wright & Filippis ("W&F"), to notify your office of a data security incident affecting approximately 45 New Hampshire residents. W&F is located at 2845 Crooks Rd., Rochester Hills, MI 48309.

On January 28, 2022, W&F was subject to a ransomware attack. With assistance from third-party experts, it took immediate steps to secure its systems and investigate the nature and scope of the Incident.

On or about May 2, 2022, W&F discovered that the Incident may have impacted protected health information ("PHI") or personally identifiable information ("PII"). On or about May 2, 2022, W&F discovered that the Incident may have impacted protected health information ("PHI") or personally identifiable information ("PII"). The Incident may have involved the following data elements for current or former patients: name, date of birth, patient number, social security number, financial account number, and/or health insurance information. Data elements for former employees and/or job applicants may have involved: name, date of birth, social security number, driver's license number or state ID, and in limited instances a financial account number.

As part of its extensive investigation, Wright & Filippis worked diligently to identify any PHI and PII that may have been subject to unauthorized access or acquisition as a result of the Incident and identify individuals to whom that PHI and PII related. This necessitated

[1] Please note that by providing this letter Wright & Filippis is not agreeing to the jurisdiction of State of New Hampshire, nor waiving its right to challenge jurisdiction in any subsequent actions.

the time- and labor-intensive process of data mining. The data mining and manual review took six full months but was ultimately necessary to properly identify potentially affected individuals.

Out of an abundance of caution, and in accordance with applicable law, W&F will provide notice to the affected New Hampshire residents so that they can take steps to minimize the risk that their information will be misused. W&F will begin sending these notices shortly to current or former patients and current or former employees or job applicants. Enclosed are the two sample notice letters. Additionally, W&F has arranged for the individuals to enroll in free credit monitoring and related services for 12 months, including identity theft insurance up to $1,000,000 as well as identity recovery and restoration services.

As set forth in the enclosed letters, W&F has taken steps to protect the security of the personal information of all individuals. Wright & Filippis endeavors to protect the privacy and security of sensitive information and has worked diligently to determine how this incident happened and are taking appropriate measures to prevent a similar situation in the future. Since the Incident, W&F has implemented a series of cybersecurity enhancements, including installation of additional endpoint detection and response software, resetting all passwords, and rebuilding affected servers.

If you require any additional information on this matter, please call me.

Sincerely,

JACKSON LEWIS, P.C.

Jackson E. Biesecker

Enclosure

WRIGHT & FILIPPIS®

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

To Enroll, Please Call:
(833) 875-0798
Or Visit:
https://response.idx.us/WrightFilippis
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

November 18, 2022

Notice of Data Breach

Dear <<FIRST NAME>> <<LAST NAME>>,

As a current or former patient of Wright & Filippis we are writing to notify you of a data incident that may have involved your protected health information and/or personal information.

What Happened

Wright & Filippis was subject to a cybersecurity attack culminating in ransomware from January 26 to January 28, 2022 (the "Incident"). Wright & Filippis' endpoint security detected and terminated the ransomware shortly after it executed. With assistance from third-party experts, Wright & Filippis took immediate steps to secure its systems and investigate the nature and scope of the Incident. On or about May 2, 2022, Wright & Filippis discovered that the Incident may have impacted protected health information ("PHI") or personally identifiable information ("PII"). We have found no evidence that your information was misused.

What Information Was Involved

Importantly, Wright & Filippis' electronic medical records were not impacted. However, the Incident may have resulted in unauthorized access to or acquisition of certain files or accounting records that may have contained one or more of the following data elements: name, date of birth, patient number, social security number, financial account number, and/or health insurance information.

What We Are Doing

As part of its extensive investigation, Wright & Filippis worked diligently to identify any PHI and PII that may have been subject to unauthorized access or acquisition as a result of the Incident and identify individuals to whom that PHI and PII related. This process was time-intensive, but ultimately necessary to properly identify potentially affected individuals.

Out of an abundance of caution, and in accordance with applicable law, we are providing this notice to you so that you can take steps to minimize the risk that your information will be misused. The attached sheet describes steps you can take to protect your identity, credit, and personal information.

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

As an added precaution, we are also offering complimentary access to identity monitoring, fraud consultation, and identity theft restoration services to help mitigate any potential for harm at no cost to you. Please see below for more information on enrollment in these services.

Wright & Filippis endeavors to protect the privacy and security of sensitive information. We have worked diligently to determine how this incident happened and are taking appropriate measures to prevent a similar situation in the future. Since the Incident we have implemented a series of cybersecurity enhancements, including installation of additional endpoint detection and response software, resetting all passwords, and rebuilding affected servers.

What You Can Do

As with any data incident, we recommend that you remain vigilant and consider taking steps to avoid identity theft, obtain additional information, and protect your personal information. Common passwords or passwords you may be using on multiple accounts should be updated to new complex passwords for added security. The attached sheet describes additional steps you can take to protect your identity and personal information.

We are offering identify theft protection services through IDX the data breach and recovery services expert. IDX identity protection services include <<12/24>> months of credit monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this specialized protection, IDX can help you resolve issues if your identity is compromised.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling (833) 875-0798 or going to https://response.idx.us/WrightFilippis and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9:00 am to 9:00 pm Eastern Time. Please note the deadline to enroll is February 18, 2023. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information. In the event this letter was addressed to a minor or to someone deceased, please call the above number and alert a representative. The services described herein can be modified accordingly.

For More Information

Please call (833) 875-0798 or go to https://response.idx.us/WrightFilippis for assistance or for any additional questions you may have. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

We sincerely apologize for this situation and any inconvenience it may cause you.

Sincerely,

Steve Filippis
President
Wright & Filippis

(Enclosure)

Recommended Steps to help Protect your Information

We recommend you remain vigilant and consider taking the following steps to avoid identity theft, obtain additional information, and protect your personal information:

- Order Your Free Credit Report at www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov. When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize and notify the credit bureaus as soon as possible in the event there are any. You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information.

- Place a Fraud Alert on Your Credit File. A fraud alert helps protect you against an identity thief opening new credit in your name. With this alert, when a merchant checks your credit history when you apply for credit, the merchant will receive a notice that you may be a victim of identity theft and to take steps to verify your identity. You also have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can place a fraud alert or request a security freeze by contacting the credit bureaus. The credit bureaus may require that you provide proper identification prior to honoring your request.

Equifax	P.O. Box 740241 Atlanta, GA 30374	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 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

- Remove your name from mailing lists of pre-approved offers of credit for approximately six months.

- If you aren't already doing so, please pay close attention to all bills and credit-card charges you receive for items you did not contract for or purchase. Review all of your bank account statements frequently for checks, purchases or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

- The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You may also obtain information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General, and/or the Federal Trade Commission ("FTC"). You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC at 1-877-IDTHEFT (1-877-438-4338), or www.ftc.gov/idtheft. The mailing address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580.

- *For District of Columbia Residents:* You can obtain additional information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 200001, 202-727-3400, www.oag.dc.gov.

- *For Maryland Residents:* You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us.

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

- *For New Mexico Residents:* You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov. In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information about New Mexico consumers obtaining a security freeze, go to http://consumersunion.org/pdf/security/securityNM.pdf

- *For New York Residents:* You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or https://ag.ny.gov/internet/resource-center; or 2) NYS Department of State's Division of Consumer Protection, (800) 697-1220 or https://dos.ny.gov/consumer-protection.

- *For North Carolina Residents:* You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.

- *For Rhode Island Residents*: You may contact and obtain information from and/or report identity theft to your state attorney general at:

  Rhode Island Attorney General's Office
  150 South Main Street
  Providence, RI 02903
  Phone: (401) 274-4400
  Website: www.riag.ri.gov

  You have the right to obtain a copy of the applicable police report, if any, relating to this incident.

WRIGHT & FILIPPIS®
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
(833) 875-0798
Or Visit:
https://response.idx.us/WrightFilippis
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

November 18, 2022

Notice of Data Breach

Dear <<FIRST NAME>> <<LAST NAME>>,

As a current or former employee or job applicant of Wright & Filippis we are writing to notify you of a data incident that may have involved your protected health information and/or personal information.

What Happened

Wright & Filippis was subject to a cybersecurity attack culminating in ransomware from January 26 to January 28, 2022 (the "Incident"). Wright & Filippis' endpoint security detected and terminated the ransomware shortly after it executed. With assistance from third-party experts, Wright & Filippis took immediate steps to secure its systems and investigate the nature and scope of the Incident. On or about May 2, 2022, Wright & Filippis discovered that the Incident may have impacted protected health information ("PHI") or personally identifiable information ("PII"). We have found no evidence that your information was misused.

What Information Was Involved

Importantly, Wright & Filippis' electronic medical records and HR system were not impacted. However, the Incident may have resulted in unauthorized access to or acquisition of certain files or accounting records that may have contained one or more of the following data elements: name, date of birth, social security number, driver's license number or state ID, and in limited instances a financial account number. Some current or former employees or applicants may have also been patients of Wright & Filippis. In this case, patient numbers and/or health insurance information may have also been affected.

What We Are Doing

As part of its extensive investigation, Wright & Filippis worked diligently to identify any PHI and PII that may have been subject to unauthorized access or acquisition as a result of the Incident and identify individuals to whom that PHI and PII related. This process was time-intensive, but ultimately necessary to properly identify potentially affected individuals.

Out of an abundance of caution, and in accordance with applicable law, we are providing this notice to you so that you can take steps to minimize the risk that your information will be misused. The attached sheet describes steps you can take to protect your identity, credit, and personal information.

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

As an added precaution, we are also offering complimentary access to identity monitoring, fraud consultation, and identity theft restoration services to help mitigate any potential for harm at no cost to you. Please see below for more information on enrollment in these services.

Wright & Filippis endeavors to protect the privacy and security of sensitive information. We have worked diligently to determine how this incident happened and are taking appropriate measures to prevent a similar situation in the future. Since the Incident we have implemented a series of cybersecurity enhancements, including installation of additional endpoint detection and response software, resetting all passwords, and rebuilding affected servers.

What You Can Do

As with any data incident, we recommend that you remain vigilant and consider taking steps to avoid identity theft, obtain additional information, and protect your personal information. Common passwords or passwords you may be using on multiple accounts should be updated to new complex passwords for added security. The attached sheet describes additional steps you can take to protect your identity and personal information.

We are offering identify theft protection services through IDX the data breach and recovery services expert. IDX identity protection services include <<12/24>> months of credit monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this specialized protection, IDX can help you resolve issues if your identity is compromised.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling (833) 875-0798 or going to https://response.idx.us/WrightFilippis and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9:00 am to 9:00 pm Eastern Time. Please note the deadline to enroll is February 18, 2023. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information. In the event this letter was addressed to a minor or to someone deceased, please call the above number and alert a representative. The services described herein can be modified accordingly.

For More Information

Please call (833) 875-0798 or go to https://response.idx.us/WrightFilippis for assistance or for any additional questions you may have. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

We sincerely apologize for this situation and any inconvenience it may cause you.

Sincerely,

Steve Filippis
President
Wright & Filippis

(Enclosure)

Recommended Steps to help Protect your Information

We recommend you remain vigilant and consider taking the following steps to avoid identity theft, obtain additional information, and protect your personal information:

- Order Your Free Credit Report at www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov. When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize and notify the credit bureaus as soon as possible in the event there are any. You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information.

- Place a Fraud Alert on Your Credit File. A fraud alert helps protect you against an identity thief opening new credit in your name. With this alert, when a merchant checks your credit history when you apply for credit, the merchant will receive a notice that you may be a victim of identity theft and to take steps to verify your identity. You also have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can place a fraud alert or request a security freeze by contacting the credit bureaus. The credit bureaus may require that you provide proper identification prior to honoring your request.

Equifax	P.O. Box 740241 Atlanta, GA 30374	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 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

- Remove your name from mailing lists of pre-approved offers of credit for approximately six months.

- If you aren't already doing so, please pay close attention to all bills and credit-card charges you receive for items you did not contract for or purchase. Review all of your bank account statements frequently for checks, purchases or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.

- The Federal Trade Commission ("FTC") offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft. You may also obtain information about fraud alerts and security freezes from the consumer reporting agencies, your state Attorney General, and the FTC. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General, and/or the Federal Trade Commission ("FTC"). You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC at 1-877-IDTHEFT (1-877-438-4338), or www.ftc.gov/idtheft. The mailing address for the FTC is: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580.

- *For District of Columbia Residents:* You can obtain additional information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 200001, 202-727-3400, www.oag.dc.gov.

- *For Maryland Residents:* You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us.

PLEASE TURN PAGE FOR ADDITIONAL INFORMATION

- *For New Mexico Residents:* You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov. In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information about New Mexico consumers obtaining a security freeze, go to http://consumersunion.org/pdf/security/securityNM.pdf

- *For New York Residents:* You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or https://ag.ny.gov/internet/resource-center; or 2) NYS Department of State's Division of Consumer Protection, (800) 697-1220 or https://dos.ny.gov/consumer-protection.

- *For North Carolina Residents:* You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov.

- *For Rhode Island Residents*: You may contact and obtain information from and/or report identity theft to your state attorney general at:

  Rhode Island Attorney General's Office
  150 South Main Street
  Providence, RI 02903
  Phone: (401) 274-4400
  Website: www.riag.ri.gov

  You have the right to obtain a copy of the applicable police report, if any, relating to this incident.