CoPilot
Provider Support Services

Via First Class Mail

January 18, 2017

Attorney General Joseph Foster
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

STATE OF NH
DEPT OF JUSTICE
2017 JAN 23 AM 11: 56

Re: Notice of possible unauthorized access of personal information

Dear Attorney General Foster:

Pursuant to N.H. Rev. Stat. § 359-C:19, *et seq.*, CoPilot Provider Support Services, Inc. ("Co-Pilot") is writing to notify you of possible unauthorized access of personal information involving 728[1] residents of your state.

CoPilot is a New York-based company doing business in your state. Among other things, CoPilot maintains a website, www.monovischcp.com, that serves as a portal for physicians across the United States, to help them determine whether insurance coverage is available for ORTHOVISC and MONOVISC injections.[2] The website was and is still used by the offices of certain physicians to make inquiries about insurance coverage for these injections and contains information about certain patients as a result of those inquiries.

On December 23, 2015, CoPilot received complaints claiming that personal information submitted to the website, including some health information, was accessible for downloading from the website. Upon discovery of the incident, CoPilot took the following actions:

- Investigated the source and scope of the incident;
- Retained and conferred with counsel;
- Notified local law enforcement;
- Retained a consultant to conduct a comprehensive review of its technical policies and procedures, including an audit of its information technology system, in order to ensure that its systems are not compromised.
    - As a result of the consultant's work, CoPilot has already taken comprehensive corrective actions to prevent a recurrence of this type of incident, including retaining a nationally renowned and independent forensic IT firm to monitor the database going forward, and to further safeguard against any future incidents.
- Retained a vendor to provide identity theft protection and, for those residents whose Social Security numbers were potentially accessed, made available credit monitoring services as well.
- Although CoPilot maintains that it is not a HIPAA-covered entity or business associate, out of an abundance of caution, CoPilot has communicated with the Office for Civil Rights of the United States Department of Health and Human Services regarding this possible unauthorized access, and has otherwise taken all necessary compliance steps pursuant to HIPAA.

As a result of the investigation and these subsequent actions, CoPilot believes that it has identified the individual who accessed CoPilot's database through unauthorized means and downloaded certain personal information, and we have concluded that the patient data was not accessible for downloading by the general public (but rather just by this one individual). Our understanding is that the law enforcement investigation supports CoPilot's conclusion about the identity of the individual responsible for the unauthorized access.

---

[1] 104 individuals had personal information potentially accessed.
[2] This same website may have been accessed through www.orthovischcp.com.

CoPilot
Provider Support Services

Again, CoPilot believes that 728 residents of your state have been affected by this incident. The categories of data of this subset of individuals that may have been improperly accessed may include names, genders, dates of birth, addresses, phone numbers, and medical insurance card information. Of that subset, 104 residents of your state also may have had their Social Security numbers improperly accessed by this individual. Even so, CoPilot has no reason to believe that any personal information was targeted, misused, accessed or disclosed in a manner that exposes any of your state's residents to any significant risk of identity theft or used by any individual in such a way as to cause any of your residents' financial harm.

Individual written notice pursuant to N.H. Rev. Stat. § 359-C:19, *et seq.* will be sent on January 18, 2017 to each of the 728 affected residents, and a model of such notice is enclosed with this letter. In addition, CoPilot will be positing the information in the notice on a website and issuing a press release as substitute notice.

Should you have any questions or need further information, please do not hesitate to contact our regulatory counsel for this matter, Colin J. Zick, Esq. of Foley Hoag LLP, 155 Seaport Blvd., Boston, MA, 02210, (617) 832-1275, czick@foleyhoag.com.

Sincerely,

Caleb DesRosiers
General Counsel

Enclosure

CoPilot
Provider Support Services

<<MemberFirstName>> <<MemberLastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

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

STATE OF NH
DEPT OF JUSTICE
2017 JAN 23 AM 11:56

Re: **Notice of Data Security Incident**

Dear <<MemberFirstName>> <<MemberLastName>>,

On behalf of CoPilot Provider Support Services, Inc. ("CoPilot"), I am writing to notify you of a data security incident that first occurred in October of 2015, which may have involved your personal information.

What Happened?

CoPilot maintains a particular website, www.monovischcp.com,[1] used by physicians to help determine whether insurance coverage is available for ORTHOVISC® and MONOVISC® injections. This website may have been used by your physician's office to make an inquiry about your insurance coverage for these injections. On December 23, 2015, CoPilot received complaints claiming that personal information submitted to the site, including health information, was accessible for downloading from the website. CoPilot immediately launched an investigation and retained a leading cybersecurity consulting firm to assist in its investigation of what occurred.

As a result of CoPilot's investigation, CoPilot believes that it identified the individual who accessed CoPilot's database through unauthorized means and downloaded certain health information, and that the data was not accessible for downloading by the general public from the website. Subsequently, CoPilot referred the matter to law enforcement. Our understanding is that the law enforcement investigation supports CoPilot's conclusion about the identity of the responsible individual.

What Information Was Involved?

The data accessed may have contained information such as your name, gender, date of birth, address, phone number, and medical insurance card information. **It is important to note that your Social Security number was not included.** No medical records, or specific diagnosis or treatment information was involved in this incident, although the fact that your information was in our database, in connection with other information, could suggest that an inquiry was made regarding whether you had insurance coverage for ORTHOVISC® or MONOVISC® injections.

What we are doing.

We are committed to protecting your information and using it in an appropriate manner. We sincerely apologize for any inconvenience this incident may cause. We are taking steps to address the situation and to further protect against a similar incident in the future, including utilizing enhanced verification, enhanced encryption and implementing increased security audit activity.

At this time, we have no reason to believe that your particular data was targeted, or misused, or that it will be further accessed or disclosed in a manner that exposes you to any significant risk of identity theft, or that it will be further accessed or disclosed. Further, CoPilot has no reason to believe that the information accessed by this individual will be used in any way to cause you financial harm.

[1] This same website may have been accessed through www.orthovischcp.com.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Identity Consultation, and Identity Restoration.

Visit **kroll.idMonitoringService.com** to enroll and take advantage of your identity monitoring services.

Membership Number: **<<Member ID>>**

To receive credit services by mail instead of online, please call 1-855-205-6948. Additional information describing your services is included with this letter. Please note, the deadline to enroll in these services is April 20, 2017.

What you can do.

Please review the enclosed "*Additional Resources*" section included with this letter. This section describes additional steps you can take to help protect yourself, 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.

Please be sure to regularly check your financial institution statements, account statements, and any other relevant accounts for possible unauthorized activity, and immediately contact your institution to report any suspicious activity.

For more information.

If you have questions, please call 1-855-205-6948, Monday through Friday from 9:00 a.m. to 6:00 p.m. Eastern Time. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Caleb DesRosiers
General Counsel, CoPilot

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

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.

Security Freeze. You have the ability to place a security freeze on your credit report.

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 to any of the three credit reporting agencies listed above. 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. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The credit reporting agencies may charge a fee to place a freeze, temporarily lift it or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.)

For Massachusetts residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is $5.

Federal Trade Commission 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 immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Kroll.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Credit Monitoring through TransUnion

You'll 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 investigator, who can help you determine if it's an indicator of identity theft.

Identity Consultation

You have unlimited access to consultation with a dedicated licensed investigator at Kroll. 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 Restoration

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

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari.

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.

CoPilot
Provider Support Services

<<MemberFirstName>> <<MemberLastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

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

STATE OF NH
DEPT OF JUSTICE
2017 JAN 2 AM 11:5

Re: **Notice of Data Security Incident**

Dear <<MemberFirstName>> <<MemberLastName>>,

On behalf of CoPilot Provider Support Services, Inc. ("CoPilot"), I am writing to notify you of a data security incident that first occurred in October of 2015, which may have involved your personal information.

What Happened?

CoPilot maintains a particular website, www.monovischcp.com,[1] used by physicians to help determine whether insurance coverage is available for ORTHOVISC® and MONOVISC® injections. This website may have been used by your physician's office to make an inquiry about your insurance coverage for these injections. On December 23, 2015, CoPilot received complaints claiming that personal information submitted to the site, including health information, was accessible for downloading from the website. CoPilot immediately launched an investigation and retained a leading cybersecurity consulting firm to assist in its investigation of what occurred.

As a result of CoPilot's investigation, CoPilot believes that it identified the individual who accessed CoPilot's database through unauthorized means and downloaded certain health information, and that the data was not accessible for downloading by the general public from the website. Subsequently, CoPilot referred the matter to law enforcement. Our understanding is that the law enforcement investigation supports CoPilot's conclusion about the identity of the responsible individual.

What Information Was Involved?

The data accessed may have contained information such as your name, gender, date of birth, Social Security number, address, phone number, and medical insurance card information. No medical records, or specific diagnosis or treatment information was involved in this incident, although the fact that your information was in our database, in connection with other information, could suggest that an inquiry was made regarding whether you had insurance coverage for ORTHOVISC® or MONOVISC® injections.

What we are doing.

We are committed to protecting your information and using it in an appropriate manner. We sincerely apologize for any inconvenience this incident may cause. We are taking steps to address the situation and to further protect against a similar incident in the future, including utilizing enhanced verification, enhanced encryption and implementing increased security audit activity.

At this time, we have no reason to believe that your particular data was targeted, or misused, or that it will be further accessed or disclosed in a manner that exposes you to any significant risk of identity theft, or that it will be further accessed or disclosed. Further, CoPilot has no reason to believe that the information accessed by this individual will be used in any way to cause you financial harm.

[1] This same website may have been accessed through www.orthovischcp.com.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Identity Consultation, and Identity Restoration.

Visit **kroll.idMonitoringService.com** to enroll and take advantage of your identity monitoring services.
Membership Number: **<<Member ID>>**

To receive credit services by mail instead of online, please call 1-855-205-6948. Additional information describing your services is included with this letter. Please note, the deadline to enroll in these services is April 20, 2017.

What you can do.

Please review the enclosed "*Additional Resources*" section included with this letter. This section describes additional steps you can take to help protect yourself, 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.

Please be sure to regularly check your financial institution statements, account statements, and any other relevant accounts for possible unauthorized activity, and immediately contact your institution to report any suspicious activity.

For more information.

If you have questions, please call 1-855-205-6948, Monday through Friday from 9:00 a.m. to 6:00 p.m. Eastern Time. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Caleb DesRosiers
General Counsel, CoPilot

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

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.

Security Freeze. You have the ability to place a security freeze on your credit report.

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 to any of the three credit reporting agencies listed above. 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. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The credit reporting agencies may charge a fee to place a freeze, temporarily lift it or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.)

For Massachusetts residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is $5.

Federal Trade Commission 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 immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Kroll

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Credit Monitoring through TransUnion

You'll 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 investigator, who can help you determine if it's an indicator of identity theft.

Identity Consultation

You have unlimited access to consultation with a dedicated licensed investigator at Kroll. 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 Restoration

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

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari.

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.