

2018 NOV 19 AM 10:30

*Law Offices*

N. Wacker Drive, Ste. 3700  
Chicago, IL  
60606-1698

312-569-1000  
312-569-3256 fax  
www.drinkerbiddle.com

CALIFORNIA

DELAWARE

ILLINOIS

NEW JERSEY

NEW YORK

PENNSYLVANIA

TEXAS

WASHINGTON D.C.

November 16, 2018

Attorney General Gordon MacDonald  
Consumer Protection and Antitrust Bureau  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

**Re: Notice of Data Breach**

Dear Attorney General MacDonald:

Please be advised that our firm, Drinker Biddle & Reath LLP, represents New York Oncology Hematology, P.C. (“NYOH” or “Company”), based in Albany, New York. For over 30 years, NYOH has been a leading provider of community-based cancer care and blood disorder services in the Albany-region. A recent IT investigation revealed that the Company was the target of a sophisticated phishing attack that may have led to the unauthorized access or use of our patients’ and employees’ personal information, including 45 New Hampshire residents.

On April 20, 2018, a phishing incident occurred through which an unauthorized user gained access to 14 employee email accounts – typically only for a few hours at most. A second incident occurred between April 21, 2018 and April 27, 2018, when one additional email account became accessible. Immediately upon discovery of the incidents, NYOH’s IT vendor, took steps to reset passwords, shutting down access to these accounts.

NYOH was subsequently notified of the suspected unauthorized access by its IT vendor on May 10, 2018. NYOH then initiated its incident response protocol to determine the scope and severity of the phishing attacks. NYOH subsequently engaged a forensic firm to review of the content of the accounts. Additionally, NYOH requested help from and is cooperating with federal law enforcement to investigate the phishing attacks.

On October 1, 2018, following a thorough analysis of the email accounts affected, the forensic firm that NYOH contracted to assess the impact determined that personal information of patients and employees were contained in some of the affected email accounts, including: names, dates of birth, home addresses, email addresses, insurance information, medical information such as test results, diagnostic codes, account numbers, and service dates. In very limited circumstances, the accounts also contained patient and employee Social Security and driver’s license numbers.

Notice of Data Breach  
November 16, 2018  
Page 2

NYOH has no knowledge of any actual access to or attempted misuse of personal information related to this incident. Out of an abundance of caution, NYOH is notifying all of its current and former patients and personnel about the phishing intrusion. Moreover, the investigation suggests that the incident did not involve a breach of information technology, firewalls, networks, and/or databases. The security surrounding these systems have not been compromised.

Since the phishing attacks were discovered, NYOH, has enhanced the security of its email systems. Steps taken include active monitoring of the affected systems, regular password resets, mandating the use of encrypted email, and implementing additional employee security training and email protocols, including those requiring the use of encrypted email for the transmission of PHI. NYOH is also reviewing and updating its policies and procedures.

NYOH plans to send the attached notification letter by mail to all current and former patients and employees potentially affected (**see Appendix A attached for a copy of the notice letter**) on November 16, 2018, which will include information about the data breach and options available to them, including an offer for 12 months of free identity theft and credit monitoring services through Experian (available at: <https://www.experianidworks.com/3bcredit>) and a dedicated toll-free hotline for any questions or concerns regarding the security breach, 1-877-753-3334. In addition, NYOH will be posting information on its website that will provide information on the breach as well as FAQs and any updates (available at: <https://newyorkoncology.com/security/>).

Please feel free to contact me at [jennifer.breuer@dbr.com](mailto:jennifer.breuer@dbr.com) or 312-569-1256 if you have any questions or concerns.

Very truly yours,



Jennifer R. Breuer

cc: Kimberly Chawgo, Compliance Manager/  
Privacy Officer  
New York Oncology Hematology, P.C.

November 16, 2018

[Recipient Full Name]  
[Street Address]  
[City, State Zip Code]

**Re: Important Security Notification. Please Read This Entire Letter.**

Dear [Recipient Full Name]:

New York Oncology Hematology (NYOH) is committed to protecting the security and confidentiality of our patients' information. Regrettably, this notice concerns an email phishing incident that may have involved some of that information. Phishing is the act of sending an e-mail falsely claiming to be an established legitimate business or personal contact in an attempt to deceive the unsuspecting recipient.

**What Happened:**

NYOH determined an unauthorized user may have gained access to several employee email accounts through a series of targeted phishing emails earlier this year. Once the phishing intrusion was identified, NYOH's information technology (IT) vendor stopped the attacks by resetting passwords to affected email accounts to immediately terminate access. While we are not aware of any actual access to or attempted misuse of protected health information or employee personal information related to this incident, we are proactively notifying NYOH patients, staff, and employees about the phishing intrusion.

**When Did This Incident Happen:**

On April 20, 2018, a phishing incident occurred through which an unauthorized user gained access to 14 employee email accounts – typically only for a few hours at most. A second incident occurred between April 21, 2018 and April 27, 2018, when one additional email account became accessible. Immediately upon discovery of the incidents, NYOH's IT vendor, took steps to reset passwords, shutting down access to these accounts.

NYOH was subsequently notified of the suspected unauthorized access by its IT vendor. NYOH initiated its incident response protocol to determine the scope and severity of the phishing attacks. NYOH hired an outside forensic firm to conduct a review of the content of the accounts.

---

**What Information Was Involved:**

On October 1, 2018, following a thorough analysis of the email accounts affected, the forensic firm that NYOH contracted to assess the impact determined that protected health information and other personal information of patients and employees were contained in some of the email accounts that were affected. The following information may have been contained in the affected email accounts: names, dates of birth, home addresses, email addresses, insurance information, medical information such as test results, diagnostic codes, account numbers, and service dates. In very limited circumstances, the accounts also contained patient and employee Social Security and driver's license numbers. **However, we have no evidence that the intruder actually accessed or misused any of this information.**

**What Is NYOH Doing To Address This Situation:**

NYOH is taking precautionary steps to ensure patient safety, privacy, and peace of mind. We want to ensure the protection of all of our patients and personnel. Accordingly, we are offering you 12 months of free identity theft and credit monitoring services through Experian, including Experian's Identity Restoration assistance and IdentityWorks<sup>SM</sup>.

NYOH has taken additional steps to remediate and enhance the security of our email systems. These include active monitoring of the affected systems, regular password resets, and implementing additional employee security training and email protocols. Finally, we requested help from and are cooperating with federal law enforcement to investigate the phishing attacks.

**How To Enroll In Free Identity Theft And Credit Monitoring Services:**

You can activate fraud detection tools available through Experian by following the steps below:

- Enroll at the Experian IdentityWorks website: <https://www.experianidworks.com/3bcredit>
- Provide your **engagement number: DB09496 [For all Non-Connecticut Residents]**
- Provide your **activation code: [Recipient's Unique Activation Code]**
- Ensure that you **enroll by: February 28, 2019 (your code will not work after this date)**

If you have questions about the Experian product or services, need assistance with identity restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-753-3334 by February 28, 2019. **Please be prepared to provide the engagement number and activation code in your letter as proof of eligibility.**

**Additional Details Regarding Your 12-Month Experian IdentityWorks Membership:**

Note, a credit card is **not** required for enrollment in Experian IdentityWorks. You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.
- **Credit Monitoring:** Actively monitors Experian, Equifax and TransUnion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 1-877-753-3334. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

**What Additional Steps You Can Take To Protect Your Information:**

There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration) for this information.

- **Call the toll-free numbers of any of the three major credit bureaus (below) to place a fraud alert on your credit report.** This can help prevent an identity thief from opening accounts in your name. You only need to contact one of the credit bureaus. As soon as that credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report, and all three reports will be sent to you free of charge.
  - **Equifax:** 1-800-525-6285; [www.equifax.com](http://www.equifax.com); P.O. Box 740241, Atlanta, GA 30374-0241.
  - **Experian:** 1-888-EXPERIAN (1-888-397-3742); [www.experian.com](http://www.experian.com); P.O. Box 9532, Allen, TX 75013.

**NYOH/Albany**  
400 Patroon Creek Blvd.  
Suite 1  
Albany, NY 12206  
(518) 489-0044

**NYOH/AMC**  
43 New Scotland Ave.  
Mail Code 7  
Albany, NY 12208  
(518) 262-6696

**NYOH/Amsterdam**  
1700 Riverfront Center  
Amsterdam, NY 12010  
(518) 843-0020

**NYOH/Clifton Park**  
3 Crossing Blvd.  
Suite 1  
Clifton Park, NY 12065  
(518) 831-4434

**NYOH/Hudson**  
69 Prospect Ave.  
Hudson, NY 12534  
(518) 822-8484

**NYOH/Rexford**  
896 Riverview Rd.  
Rexford, NY 12148  
(518) 399-4600

**NYOH/Troy**  
258 Hoosick St.  
Suite 206  
Troy, NY 12180  
(518) 272-2097

- **TransUnion:** 1-800-680-7289; [www.transunion.com](http://www.transunion.com); Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.
- **Monitor your credit reports and other accounts.** Even though you are being provided credit monitoring services, you should continue to monitor your credit reports to ensure an imposter has not opened an account with your personal information. You also should closely monitor your financial and other account statements, and if you notice any unauthorized activity, promptly contact the creditor.
- **Contact law enforcement if you find suspicious activity.** If you find suspicious activity on your credit reports or other account information, contact your local police department and file a report of identity theft. Keep copies of such reports for your records, as you may need to give them to creditors.
- **Other resources.** For more information about steps you can take to avoid identity theft, you may contact the Federal Trade Commission, by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington DC, 20580, via the Internet at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft) or by phone at 1-877-ID-THEFT (1-877-438-4338).

We apologize and deeply regret that this incident occurred. Please know that we take your privacy and security very seriously. That is why we have set up a dedicated toll-free number to call with questions related to this incident: **1-877-753-3334**. It is available Monday-Friday, from 9am ET to 9pm ET and Saturday-Sunday, 11am ET to 8pm ET. You may also visit: <https://newyorkoncology.com/security> for additional information and updates.

Sincerely,



Ira Zackon, MD  
President  
New York Oncology Hematology