

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

<<Date>>

**Re: Notice of Data <<Security Incident/Breach>>**

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

We are writing to provide you with information about a recent data security incident that involved your personal and protected health information. While you may not have heard of Von Behren & Hunter LLP (“VBH”), we are a law firm that provides legal representation and consultation services to many health plans, including <<CoveredEntity>>. Please be assured that this incident did not involve the <<CoveredEntity>> network or information systems. VBH takes the privacy and security of protected health information very seriously. That is why we are notifying you of the incident and informing you about steps you can take to help protect your information.

**What Happened?** On January 24, 2022, VBH became aware of unusual activity within its network and discovered that there had been unauthorized access to the environment. Upon discovering this activity, we took steps to secure our environment and initiate an initial investigation to evaluate the scope of the incident. On February 10, 2022, VBH confirmed that certain data was accessed and acquired without authorization during the incident. Following an in-depth and thorough review, on March 25, 2022, we determined that some of your information may have been stored on the impacted server. While there is no evidence indicating that your information was accessed or acquired without authorization, we are sending this notification out of an abundance of caution.

**What Information Was Involved?** The information that may have been impacted includes your name, <<DataElements>>.

**What We Are Doing.** As soon as VBH discovered the incident, we took the measures described above. We also reviewed and enhanced our systems to reduce the likelihood of a similar incident occurring in the future. In addition, VBH has been in communication with the Federal Bureau of Investigation and will continue to cooperate with any investigation into the incident.

**What Can You Do?** You can follow the recommendations included with this letter to help protect your information. Additionally, we encourage you to contact IDX with any questions and to enroll in free identity protection services by calling <<Toll Free Number>> or going to <<Enrollment Site>> and using the Enrollment Code provided above. Representatives are available between X:00am to X:00pm <<Time Zone>> from Monday to Friday. Please note that the deadline to enroll is <<Enrollment Deadline>>.

**For More Information:** Further information about how to protect your personal information is included with this letter. If you have questions or need assistance, please contact <<Toll Free Number>>, Monday through Friday, X:00 am to X:00 pm <<Time Zone>>. Our representatives are fully versed on this incident and can answer any questions you may have regarding the protection of your personal information.

We take this matter very seriously and deeply regret any worry or inconvenience that this may cause you.

Sincerely,

William E. von Behren  
of VON BEHREN & HUNTER LLP

## 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](http://www.equifax.com)

**Experian**

P.O. Box 9532  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

**TransUnion**

P.O. Box 1000  
Chester, PA 19016  
1-800-916-8800  
[www.transunion.com](http://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 Rhode Island Attorney General**

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

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>.