



Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Patrick H. Haggerty
direct dial: 513.929.3412
phaggerty@bakerlaw.com

April 19, 2022

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

Brian E. Frosh
Attorney General
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Incident Notification

Dear Attorney General Frosh:

We are writing on behalf of our client, Baum Sigman Auerbach & Neuman, Ltd. (“Baum Sigman”), to notify your office of a cybersecurity incident that occurred at Baum Sigman that involved one Maryland residents’ personal information that it received from its client, UNITE HERE HEALTH.¹

Baum Sigman is a law firm located in Chicago, Illinois, that provides legal services to UNITED HERE HEALTH. Baum Sigman recently concluded an investigation into suspicious activity originating from two Baum Sigman employee email accounts. As soon as Baum Sigman became aware of the activity, they immediately took measures to secure the email accounts and launched an investigation with the assistance of a cybersecurity firm. The investigation determined that an unauthorized person accessed the employee email accounts at various times between August 19, 2021 and October 4, 2021, but it was not able to determine whether any specific emails or attachments were accessed or downloaded by the unauthorized person. However, Baum Sigman was not able to rule out that possibility. Baum Sigman, therefore, searched and reviewed the emails and attachments that could have been accessed or downloaded, and determined on March 4, 2022, that an email or attachment contained a Maryland residents’ name, Social Security number, eligibility and contribution related information. Thereafter, on March 29, 2022, Baum Sigman notified UNITE HERE HEALTH that a Maryland resident’s personal information was involved in the incident.

¹ UNITE HERE HEALTH is a covered entity under the Health Insurance Portability & Accountability Act (“HIPAA”) and Baum Sigman is a business associate of UNITE HERE HEALTH.

April 19, 2022

Page 2

Beginning today, Baum Sigman will mail a notification letter to the Maryland resident via U.S. First-Class mail in accordance with Md. Code Ann., Com. Law § 14-3504.² A sample copy of the notification letter is enclosed. Baum Sigman is offering the Maryland resident whose Social Security number is involved one year of complimentary credit monitoring, fraud consultation, and identity theft restoration services through Kroll.

To reduce the risk of a similar incident from occurring in the future, Baum Sigman is enhancing already existing electronic security protocols and are providing additional security awareness training for all staff.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



Patrick H. Haggerty
Partner

Enclosure

² This report does not waive Baum Sigman's objection that Maryland lacks regulatory authority over it related to any claims that may arise from this incident.

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

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

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Baum Sigman Auerbach & Neuman, Ltd. is a law firm that provides legal services to UNITE HERE HEALTH. I am writing to inform you of an incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you may consider taking.

We recently concluded an investigation into suspicious activity originating from two Baum Sigman employee email accounts. As soon as we became aware of the activity, we immediately took measures to secure the email accounts and launched an investigation with the assistance of a cybersecurity firm. The investigation determined that an unauthorized person accessed the employee email accounts at various times between August 19, 2021 and October 4, 2021, but it was not able to determine whether any specific emails or attachments were accessed or downloaded by the unauthorized person. However, we were not able to rule out that possibility. Out of an abundance of caution, we reviewed all emails and attachments that could have been accessed or downloaded. We determined on March 4, 2022, that an email or attachment contained your <<b2b_text_1 (Impacted Data)>>. Thereafter, on March 29, 2022, we notified UNITE HERE HEALTH that your information was involved in the incident.

While we believe that the unauthorized access occurred as part of an attempt to obtain money through a wire transfer and not to access personal information, we encourage you to remain vigilant by reviewing your account statements and credit reports for any unauthorized activity. If you see charges or activity you did not authorize, please contact your financial institution immediately. As an added precaution, we are offering you a complimentary one-year membership to Kroll 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 <<b2b_text_6 (Activation Date)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.

Additional information describing your services is included with this letter.

We sincerely regret any inconvenience or concern this incident may cause. To further protect personal information, we have taken additional steps to enhance our existing electronic security protocols and are providing additional security awareness training for our staff. If you have any questions, please call 1-855-482-1572, Monday through Friday from 8:00 A.M. through 5:30 P.M. Central Time, excluding major U.S. holidays.

Sincerely,

A handwritten signature in black ink, appearing to read "Laura M. Finnegan". The script is fluid and cursive, with the first name "Laura" being more prominent.

Laura M. Finnegan



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—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.

Additional Steps You Can Take

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any 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 companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

If your health insurance or medical information was involved, it is also advisable to review the billing statements you receive from your health insurer or healthcare provider. If you see charges for services you did not receive, please contact the insurer or provider immediately.

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Baum Sigman Auerbach & Neuman, Ltd.'s mailing address is 200 W Adams St Ste 2200, Chicago, IL 60606 and its phone number is 312-236-4316.

Additional information for residents of the following states:

Maryland: You may contact and obtain information from your state attorney general at: Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>