11/14/2022

To whom it may concern,

This letter serves as notification that personal health information ("PHI") may have been compromised during a data breach that occurred recently at Barran Liebman LLP ("Barran Liebman"), a law firm that CODA, Inc. ("CODA") uses to assist with employment issues. The information exposed by the breach is not financial information and does not include any social security numbers, credit card numbers, bank account numbers, passwords, or other ways a person could get into a financial account or find out related data. We are sending this notice because both CODA and Barran Liebman want you to be aware of any events that may affect your privacy.

On October 7, 2022, CODA learned that an unauthorized individual (the "intruder") was able to get inside the computer systems at Barran Liebman on August 19, 2021. While inside the system, the intruder accessed a specific group of files. One large file contained documents involving seven CODA patients. First and last names, and the fact that these individuals were receiving treatment at CODA, were included with other, non-patient related information, in this file.

After learning of the breach, Barran Liebman immediately limited the intruder's ability to access information on their system and began to investigate. As part of the investigation, they engaged cybersecurity professionals to analyze the incident and to determine if anyone's personal data was involved. They reviewed every record accessed by the intruder to see if any contained personally identifiable information.

We don't believe any patients were a target in this incident, and the intruder may not have viewed or taken patient data. To date, we have no reports of identity theft, fraud, or other unauthorized use of patient information. Barran Liebman reports that their cybersecurity professionals have not found any of the affected patient information on the dark web or anywhere else. Because we have been unable to reach former patients by mail, we are posting this notification so any affected individuals can take steps to protect your privacy. The document attached to this letter describes specific steps you can take to protect your personal information.

If you have any questions about this incident, please call Barran Liebman at (855) 926-1350. This is a dedicated, confidential, toll-free phone number. It is open Monday through Friday from 6:00 am to 3:30 pm Pacific Time, excluding major US holidays. It is staffed with professionals who are familiar with the incident and can help you protect your information and identity.

At CODA, the privacy of your information is a top priority. We take this incident very seriously and deeply regret any problems or worry this incident may cause you. We are working with Barran Liebman to make sure that their safeguards meet legal standards to protect your personal information.

Very truly yours,

Alison Noice, MA, MS, CADC III
Executive Director

Attachment A

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion LLC
P.O. Box 6790
Fullerton, PA 92834-6790
https://www.transunion.com/fraud-alerts
(800) 680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
http://www.transunion.com/creditfreeze
1-888-909-8872

In order to place the security freeze, 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 reporting company will send you a confirmation letter containing 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.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

4. Protecting Your Medical Information.

We have no evidence that your medical information involved in this incident was or will be used for any unintended purposes. However, the following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.