大成 DENTONS BINGHAM GREENEBAUM

Kyle W. Miller

kyle.miller@dentons.com
D +1 502 587 3517

Dentons Bingham Greenebaum LLP
3500 PNC Tower
101 South Fifth Street
Louisville, KY 40202
United States

dentons.com

May 22, 2023

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Re: Notice of Data Breach

Attorney General Brenna Bird,

We write pursuant to Iowa Code § 715C.1, et seq. to inform you that Apria Healthcare LLC ("Apria") will be sending a notice to Iowa residents advising them of a security incident. On September 1, 2021 Apria received a notification regarding access to select Apria systems by an unauthorized third-party. The unauthorized third party accessed systems which contained personal information from April 5, 2019 to May 7, 2019 and from August 27, 2021 to October 10, 2021. Apria took immediate action to mitigate the incident, including working with the Federal Bureau of Investigation and hiring a reputable forensic investigation team to investigate and securely resolve the incident.

Based on the investigation and discussions with law enforcement, Apria believes the purpose of the unauthorized access was to fraudulently obtain funds from Apria, and not to access personal information of its patients or employees. There is no evidence of funds removed, and Apria is not aware of the misuse of personal information related to this incident. A small number of emails and files were confirmed to have been accessed, but there is no proof that any data was taken from any system. For the individuals receiving this notice, the investigation was unable to confirm whether any emails or files about them were actually accessed. The information potentially accessed in the incident varied for each individual and may have included personal, medical, health insurance or financial information, and in some limited cases, Social Security numbers.

Apria has implemented additional security measures upon the guidance and recommendation of our forensic investigators to help prevent the reoccurrence of a similar breach and to further protect the privacy of our patients and employees.

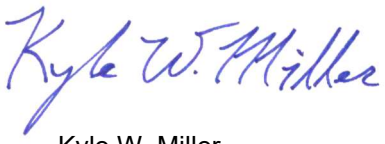
As a precautionary measure, we have arranged for impacted individuals to enroll in identity protection services from Kroll; which includes credit monitoring, fraud consultation, and identity theft restoration; this service will be offered at no cost for at least 12 months.

A formal notice of the incident will be sent in the coming weeks by U.S. mail to the individuals for whom we have identified a mailing address. A copy of the anticipated notice is attached. We alerted all others via a national press release and information on our web site on May 22, 2023. Details for enrollment will

be included in the notification letter received by those who are potentially affected or who call in to the call-center referenced in the notification letter or press release.

Please contact me if you have any questions.

Sincerely,



Kyle W. Miller

KWM:

Enclosure

<<MemberFirstName>> <<MemberLastName>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip Code>>

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

Notice of Data Breach

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

We are writing to tell you about a data breach that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

What happened?

On September 1, 2021, Apria Healthcare LLC ("Apria") received a notification regarding access to select Apria systems by an unauthorized third party. Apria took immediate action to mitigate the incident, including working with the Federal Bureau of Investigation (FBI) and hiring a reputable forensic investigation team to investigate and securely resolve the incident. An unauthorized third party accessed systems which contained personal information from April 5, 2019 to May 7, 2019 and from August 27, 2021 to October 10, 2021.

What information was involved?

Based on its investigation and discussions with law enforcement, Apria believes the purpose of the unauthorized access was to fraudulently obtain funds from Apria and not to access personal information of its patients or employees. There is no evidence of funds removed, and Apria is not aware of the misuse of personal information related to this incident. A small number of emails and files were confirmed to have been accessed, but there is no proof that any data was taken from any system. For the individuals receiving this notice, the investigation was unable to confirm whether any emails or files about you were actually accessed. Therefore, Apria has identified the following information relating to you that may have been accessed by the attacker: <<VText>>.

What we are doing.

Apria has worked with the FBI and forensic investigators to conduct a thorough review of the potentially affected systems. We have also implemented additional security measures upon the guidance and recommendation of our forensic investigators to help prevent the reoccurrence of a similar breach and to further protect the privacy of our patients and employees.

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, Fraud Consultation, and Identity Theft Restoration.

Visit **<<IDMonitoringURL>>** to activate and take advantage of your identity monitoring services.

*You have until **<<Date>>** to activate your identity monitoring services.*

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

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

Additional information describing your services is included with this letter.

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.

For more information.

If you have questions, please call (866) 347-6672, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

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,

Doreen Bellucci

Senior Vice President, General Counsel & Secretary

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

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 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. 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 Alerts. There are two types of 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 at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

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 use an online process, an automated telephone line, or submit 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 5 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, and display your name, current mailing address, and the date of issue.

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 minimize the risks of 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.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

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

Single Bureau Credit Monitoring

You will 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 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.