

Jason M. Schwent
T (312) 985-5939
Email:jschwent@clarkhill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

April 25, 2024

VIA ELECTRONIC MAIL

Attorney General Anthony Brown
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Dear Attorney General Brown:

We represent Berry, Dunn, McNeil & Parker, LLC (“BerryDunn”) with respect to a data security incident involving the potential exposure of certain personally identifiable information (“PII”) described in more detail below. BerryDunn, an accounting, assurance, and consulting firm located in Bangor, ME, is providing this notice on behalf of its covered entity clients. BerryDunn is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident from occurring in the future.

1. Nature of security incident.

On September 14, 2023, BerryDunn was notified that one of its vendors, ZZ Enterprises, LLC, d/b/a Reliable Networks (“Reliable”), a managed service provider of BerryDunn’s Health Analytics Practice Group (“HAPG”), had discovered suspicious network activity that was impacting its network, including systems it managed on behalf of HAPG. BerryDunn immediately implemented its incident response protocols, and engaged cybersecurity experts to assist with determining what occurred and whether any data was compromised. The investigation found that an unauthorized actor gained access to Reliable’s network and took some data stored on the HAPG systems. BerryDunn engaged a vendor to conduct an in-depth review of the impacted data to determine what personal information may have been impacted and identify any individuals for whom the personal information belongs. This review was completed on April 2, 2024. From this review, it appears that some combination of individuals’ names, addresses, dates of birth, Social Security numbers, health insurance policy numbers, Medicare or Medicaid numbers, state or governmental ID numbers, passport numbers, and limited medical information was contained in the impacted data.

2. Number of residents affected.

Thirty-five (35) Maryland residents may have been affected and were notified of the incident. A notification letter was sent to the potentially affected individuals on April 25, 2024. A copy of the form notification letter is enclosed.

3. Steps taken in response.

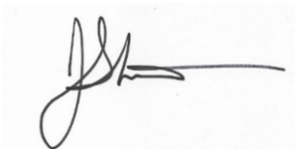
Since this incident, BerryDunn has taken steps to secure the HAPG data, such as decommissioning all BerryDunn systems under Reliable's control and migrating all HAPG data to secure internal BerryDunn systems that are continually monitored as part of our cybersecurity program. In addition, impacted individuals were offered 12 months of credit monitoring and identity protection services through IDX.

4. Contact information.

BerryDunn takes the security of the information in its control seriously and is committed to ensuring it is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at jschwent@clarkhill.com or (312) 985-5900.

Sincerely,

CLARK HILL

A handwritten signature in black ink, appearing to read 'JS', followed by a long horizontal line extending to the right.

Jason M. Schwent



PO Box 480149
Niles, IL 60714

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

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

April 11, 2024

Notice of Data Security Incident

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

Berry, Dunn, McNeil & Parker, LLC (“BerryDunn”) is writing to notify you of a recent data security incident experienced by a vendor of BerryDunn’s, Health Analytics Practice Group (“HAPG”) that may have impacted your personal information. HAPG receives personal information from its clients to provide data analytics services. We take the privacy and security of your information seriously and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information and resources we are making available to you.

What Happened

On September 14, 2023, BerryDunn was notified that one of its vendors, Reliable Networks of Maine, LLC (“Reliable”), who is a managed service provider for HAPG, had discovered suspicious network activity that was impacting its network, including systems it managed on behalf of HAPG. BerryDunn immediately implemented its incident response protocols, and engaged cybersecurity experts to assist with determining what occurred and whether any data was compromised. The investigation found that an unauthorized actor gained access to Reliable’s network and took some data stored on the HAPG systems. BerryDunn then hired a vendor to conduct an in-depth review of the impacted data to determine what personal information may have been impacted and identify any individuals for whom the personal information belongs. This review was completed on April 2, 2024.

While we have no evidence that your personal information was misused, we wanted to inform you about this incident out of an abundance of caution.

What Information Was Involved

The impacted information may include a combination of the following: your name, address, <<Variable Text>>.

What We Are Doing

BerryDunn has taken steps to secure the HAPG data, such as decommissioning all BerryDunn systems under Reliable’s control and migrating all HAPG data to secure internal BerryDunn systems that are continually monitored as part of our cybersecurity program.

In addition, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: <<12 months/24 months>> of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

Please review the enclosed Recommended Steps 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. You should also regularly review your credit reports and financial statements, and immediately report any suspicious activity.

We also encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling (888) 817-7503 or going to <https://app.idx.us/account-creation/protect> or scanning the QR code and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is July 17, 2024.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

You will find detailed instructions for enrollment on the enclosed Recommended Steps section of this letter. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

For More Information

If you have questions, please call (888) 817-7503, Monday through Friday from 9 am - 9 pm Eastern Time or go to <https://app.idx.us/account-creation/protect> for assistance. Your trust is a top priority for us, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Berry, Dunn, McNeil & Parker, LLC

Berry, Dunn, McNeil & Parker, LLC



Recommended Steps to help Protect your Information

1. Website and Enrollment. Scan the QR code or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at (888) 817-7503 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

District of Columbia Residents: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Iowa Residents: Office of the Attorney General, 1305 E. Walnut Street, Des Moines, Iowa 50319; 515-281-5926; consumer@ag.iowa.gov.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400. Total Rhode Island residents notified is <<XX>>.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.