SpencerFane

March 21, 2024

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification of Data Security Incident

To Whom it May Concern:

We are writing on behalf of M&D Capital Premier Billing LLC and the related entities ASC Strategic Services LLC and Drachman Katz LLP (M&D) in connection with the data security incident described below. M&D provides medical billing and related services to medical providers and has a principal address of 115-06 Myrtle Avenue, Richmond Hill, NY 11418.

On or around July 8, 2023, M&D Capital Premier Billing LLC ("M&D") identified suspicious activity within its computer environment. M&D immediately took steps to secure its network and launched an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the activity. Through the investigation, M&D determined that an unauthorized threat actor may have had access to certain systems beginning on or around June 20, 2023. As a result, certain files within M&D's systems may have been accessed or acquired by the unauthorized threat actor. During its investigation, M&D decided to notify all its covered entity clients of this incident on January 10, 2024. Because of the nature of the incident and the potentially impacted data, M&D did not have a clear understanding of who may have been impacted by this incident until February 23, 2024.

The impacted systems contained demographic and healthcare information provided by the M&D covered entity clients, which included

Upon learning of the malicious activity, M&D promptly notified federal law enforcement and took steps to further secure its systems and investigate the event. M&D reviewed its existing policies and procedures and implemented additional administrative and technical safeguards to help prevent future attacks. M&D also worked with third-party subject matter specialists to further enhance the security of its systems.

Additionally, M&D is providing affected individuals with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services and proactive fraud assistance at no charge. These services will be provided by Cyberscout through Identity Force, a

SpencerFane

TransUnion company specializing in fraud assistance and remediation services.

M&D mailed notification letters to 25 residents of your state on March 21, 2024, on behalf of 27 M&D covered entity clients. A sample copy of the notification letter is enclosed.

Respectfully,
Spencer Fane, LLP

Shawn E. Tuma, Partner

Enclosures: Notice of Data Breach

M&D Capital Premier Billing LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

M&D Capital Premier Billing LLC
115-06 Myrtle Avenue
Richmond Hill, NY 11418

[redacted]

March 18, 2024

Notice of Data Breach

Dear [redacted],

What Happened

M&D Capital Premier Billing LLC ("M&D") writes on behalf of each M&D Entity and Impacted Covered Entity listed below to inform you of an incident that involved your personal information.

M&D ENTITY	IMPACTED COVERED ENTITY
[redacted]	[redacted]

On or around July 8, 2023, we identified suspicious activity within our computer environment. We immediately took steps to secure our network and launched an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the activity. Through the investigation, we determined that an unauthorized threat actor may have had access to certain systems beginning on or around June 20, 2023. As a result, certain files within our systems may have been accessed or acquired by the unauthorized threat actor. Based on the investigation we determined that your data may have been included on the impacted systems.

What Information Was Involved

The impacted systems contained demographic and healthcare information provided by the Covered Entity, which may include your name, address, medical billing and insurance information, certain medical information such as diagnoses, medication and treatments, and demographic information such as date of birth, Social Security number and financial information.

What We Are Doing

We take the confidentiality, privacy, and security of information in our possession seriously. Upon learning of the malicious activity, we promptly notified law enforcement and took steps to further secure our systems and investigate the event. As part of our ongoing commitment to the privacy of personal information in our care, we reviewed our existing policies and procedures and implemented additional administrative and technical safeguards to help prevent future attacks. We also worked with third-party subject matter specialists to further enhance the security of our systems.

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to https://secure.identityforce.com/benefit/mdcpb and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What You Can Do

The events that have occurred do not automatically mean that you are a victim of identity theft. However, we encourage you to remain vigilant and to continually review your healthcare insurance information. Additionally, you should continually review your credit report, bank account activity, and bank statements for irregularities or unauthorized items, and to immediately report any unauthorized charges to your financial institution. We also encourage you to enroll in the free identity protection services.

Who is M&D and the M&D Entities?

M&D and the M&D Entities provides medical billing and related services to medical providers. If you received this letter, M&D provides services to one of your medical providers.

For More Information

You will find additional information on the enclosed Protect Your Information document.

We value your privacy and sincerely regret any inconvenience this matter may cause. Your confidence in our ability to safeguard your personal information and your peace of mind are very important to us.

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-844-794-1844 and supply the fraud specialist with your unique code listed above.

Sincerely,

M&D Capital Premier Billing LLC

Protect your Information

1. 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.

2. Law Enforcement. 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.

3. 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	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.alerts.equifax.com	www.experian.com	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.

4. 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.
Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II,III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, ere.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

5. 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, at https://www.identitytheft.gov/.

California Residents: Visit the California Office of Privacy Protection (http://www.ca.gov/Privacy) for additional information on protection against identity theft.

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.

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: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400.

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