
Kutak Rock LLP
1650 Farnam St.
Omaha, NE 68102

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

December 10, 2020

**Notice of Data Breach**

Dear Family of <<Name 1>>:

We are writing to make you aware of a recent privacy issue at Midwest Geriatric Management, LLC ("MGM"). We take patient privacy very seriously and understand that your personal information is important to you.

**What Happened**

A fraudster recently mimicked the email account of our CFO and sent an email to an MGM employee, requesting that a spreadsheet be emailed to him. Although our email system has built in security features that help block such attempts, this particular email was written in a way that circumvented those security measures. The employee unfortunately emailed some of the requested information to the fraudster, mistakenly believing he was sending the spreadsheet to the legitimate CFO. The spreadsheet contained certain personal information. You are receiving this notice because we believe some personal information was included in the spreadsheet.

**What Information Was Involved**

The spreadsheet contained the following information:

1. Name
2. Account balance, if applicable
3. The name of the relevant facility

**What We Did and What We Are Doing**

As soon as MGM discovered what happened, we immediately began investigating. We contacted our IT provider to analyze the entire network and our CFO's email account. This review confirmed there was no breach or infiltration of the system or any other suspicious activity. We performed

other tests on the CFO's mailbox, which turned up nothing unusual. In short, this was an isolated incident and did not involve any other data on MGM's system. We have reiterated our training with the affected employee and all employees about being mindful of emails coming from outside MGM.

We take our responsibility to safeguard your personal information seriously. We are sorry this happened. In the interest of protecting our patients, we are offering *my*TrueIdentity identity theft protection services through TransUnion Interactive at no cost to you. *my*TrueIdentity services include: 12 months of credit monitoring, unlimited TransUnion Report & Score access, and a $1,000,000 insurance reimbursement policy. With this protection, *my*TrueIdentity will help you resolve issues if your identity is compromised. We have no evidence to suggest that your information has been misused at this time, but we encourage you to take full advantage of these identity theft protection services. You can contact TransUnion Interactive and enroll by calling **1-855-288-5422** or going to **www.MyTrueIdentity.com** and using the Enrollment Code provided above. You will have unlimited, toll-free access to *Identity Protection Specialists*. Please note the deadline to enroll is March 31, 2021. Please do not discard this letter: you will need to reference the enrollment code at the top of this letter when calling or enrolling online. We have also included additional information in the Recommended Steps below with contact information for the three major credit bureaus and select government agencies.

**What You Can Do**

We encourage you to contact TransUnion Interactive to enroll in the free *my*TrueIdentity services by calling 855-288-5422 or going to **www.MyTrueIdentity.com** and using the Enrollment Code provided above. We encourage you to take full advantage of this service offering and reach out to Midwest Geriatric with any questions and concerns.

There are additional actions you can consider taking to reduce the risk of identity theft or fraud on your account(s). Please refer to the enclosed Recommended Steps document for more information.

**For More Information**

You will find detailed instructions for enrollment on the enclosed document. 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.

Please call 855-288-5422 or go to **www.MyTrueIdentity.com** for assistance with any additional questions you may have about enrolling in *my*TrueIdentity services.

If you have any questions about the underlying incident, please feel free to call (402) 231-8968.

Sincerely,

Judah Bienstock
CEO


Kutak Rock LLP
1650 Farnam St.
Omaha, NE 68102

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

December 10, 2020

**Notice of Data Breach**

Dear Family of <<Name 1>>:

We are writing to make you aware of a recent privacy issue at Midwest Geriatric Management, LLC ("MGM"). We take patient privacy very seriously and understand that your personal information is important to you.

## What Happened

A fraudster recently mimicked the email account of our CFO and sent an email to an MGM employee, requesting that a spreadsheet be emailed to him. Although our email system has built in security features that help block such attempts, this particular email was written in a way that circumvented those security measures. The employee unfortunately emailed some of the requested information to the fraudster, mistakenly believing he was sending the spreadsheet to the legitimate CFO. The spreadsheet contained certain personal information. You are receiving this notice because we believe some personal information was included in the spreadsheet.

## What Information Was Involved

The spreadsheet contained the following information:

1. Name
2. Account balance, if applicable
3. Social Security Number
4. The name of the relevant facility

## What We Did and What We Are Doing

As soon as MGM discovered what happened, we immediately began investigating. We contacted our IT provider to analyze the entire network and our CFO's email account. This review confirmed

there was no breach or infiltration of the system or any other suspicious activity. We performed other tests on the CFO's mailbox, which turned up nothing unusual. In short, this was an isolated incident and did not involve any other data on MGM's system. We have reiterated our training with the affected employee and all employees about being mindful of emails coming from outside MGM.

We take our responsibility to safeguard your personal information seriously. We are sorry this happened. In the interest of protecting our patients, we are offering *my*TrueIdentity identity theft protection services through TransUnion Interactive at no cost to you. *my*TrueIdentity services include: 12 months of credit monitoring, unlimited TransUnion Report & Score access, and a $1,000,000 insurance reimbursement policy. With this protection, *my*TrueIdentity will help you resolve issues if your identity is compromised. We have no evidence to suggest that your information has been misused at this time, but we encourage you to take full advantage of these identity theft protection services. You can contact TransUnion Interactive and enroll by calling **1-855-288-5422** or going to **www.MyTrueIdentity.com** and using the Enrollment Code provided above. You will have unlimited, toll-free access to *Identity Protection Specialists*. Please note the deadline to enroll is March 31, 2021. Please do not discard this letter: you will need to reference the enrollment code at the top of this letter when calling or enrolling online. We have also included additional information in the Recommended Steps below with contact information for the three major credit bureaus and select government agencies.

**What You Can Do**

We encourage you to contact TransUnion Interactive to enroll in the free *my*TrueIdentity services by calling 855-288-5422 or going to **www.MyTrueIdentity.com** and using the Enrollment Code provided above. We encourage you to take full advantage of this service offering and reach out to Midwest Geriatric with any questions and concerns.

There are additional actions you can consider taking to reduce the risk of identity theft or fraud on your account(s). Please refer to the enclosed Recommended Steps document for more information.

**For More Information**

You will find detailed instructions for enrollment on the enclosed document. 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.

Please call 855-288-5422 or go to **www.MyTrueIdentity.com** for assistance with any additional questions you may have about enrolling in *my*TrueIdentity services.

If you have any questions about the underlying incident, please feel free to call (402) 231-8968.

Sincerely,

Judah Bienstock

TransUnion

CEO

**ACTIVATION CODE: XXXXXXXXXXX X**

## Complimentary One-Year *my*TrueIdentity Credit Monitoring Service

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

**HOW TO ENROLL: YOU CAN SIGN UP ONLINE OR VIA U.S. MAIL DELIVERY**

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **XXXXXXXXXXXX** and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **XXXXXX** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **March 31, 2021.** Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

**ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:**

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

**ADDITIONAL RECOMMENDED STEPS TO HELP PROTECT YOUR INFORMATION**

In addition to enrolling in *my*TrueIdentity Credit Monitoring Services, you can also take the following steps to help guard against fraud and identity theft:

**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.

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

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.

**2. 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.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.**

**3. 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.

**4. 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.

**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**,** Consumer Protection Division, 9001 Mail Service Center**,** Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6000 and 877-5-NO-SCAM (toll free in North Carolina)

**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.