Mid-Minnesota Management Services d/b/a Central Resources
2700 1st Street North, Suite 303
St. Cloud, MN 56303

Postal Endorsement Line
<<Full Name>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

<<Date>>

Dear <<Full Name>>,

We are contacting you to notify you that Mid-Minnesota Management Services d/b/a Central Resources experienced a security incident through one of our downstream vendors that may have involved your personal information. Central Resources was acting as a debt collector for our client <<Business Name>>. RAYUS Radiology was not directly involved with this incident, but made all attempts to mitigate immediately upon learning of the event.

WHAT HAPPENED?

A subcontractor's vendor inadvertently released a file containing your protected health information in a text message on September 12, 2024. After some messages were sent, the vendor recognized the mistake and stopped the campaign. One of our clients contacted the entire list of potential recipients by text on September 13, 2024 and requested that each delete this inadvertent file transfer. The downstream vendor is no longer providing services on any of our matters.

WHAT INFORMATION WAS INVOLVED?

We informed our clients, your health care providers for which we collect outstanding payments, about this event and what personal information may have been accessed. The personal information that was accessed included **only** your name, cell number and the fact that you had an outstanding medical debt with our client. **No other information was included.**

WHAT ARE WE DOING?

Upon discovering the incident, we promptly launched an investigation. Additionally, we are working diligently to evaluate our suppliers' security processes to further strengthen the security of our processes regarding protected health information.We are working with our vendors that receive protected health information to confirm that they implement reasonable and appropriate safeguards to protect it.

WHAT CAN YOU DO?

We are notifying you so that you can take action which will assist to minimize or eliminate potential harm. We strongly advise you to take preventive measures to help prevent and detect any misuse of your information.

To help protect you, we have retained CyEx, a specialist in identity theft prevention to provide you with <<12/24>> months of credit monitoring services and identity theft services, free of charge. You can enroll in the program by following the attached directions.

As a first step, we recommend that you closely monitor your health accounts and if you see any unauthorized activity, you should promptly contact your health insurance carrier.

To further protect yourself from the possibility of identity theft, we recommend that you immediately place a fraud alert on your credit files. A fraud alert conveys a special message to anyone requesting your credit report that you suspect you were a victim of fraud. When you or someone else attempts to open a credit account in your name, the lender should take measures to verify that you have authorized the request. A fraud alert should not stop you from using your existing credit cards or other accounts, but it may slow down your ability to get new credit. An initial fraud alert is valid for ninety (90) days. To place a fraud alert on your credit reports, contact one of the three major credit reporting agencies at the appropriate number listed below or via their website. One agency will notify the other two on your behalf. You will then receive letters from the agencies with instructions on how to obtain a free copy of your credit report from each.

- Equifax (888)766-0008 or www.fraudalert.equifax.com
- Experian (888) 397-3742 or www.experian.com
- TransUnion (800) 680-7289 or www.transunion.com

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 reports periodically can help you spot a problem and address it quickly.

We sincerely apologize for the inconvenience this incident has caused you. Please be advised that we will keep you informed of any developments in the investigation which may be of importance to you.

Who to call or contact with questions?

If you have further questions or concerns, please contact Identity Defense at 855-285-9449.

Sincerely,

Central Resources Accounts Management Team

Identity Defense

Enter your Activation Code: **<<Activation Code>>**
Enrollment Deadline: **<<Enrollment Deadline>>**
Service Term: <<12/24>> months*

Identity Defense Complete

Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- $1 Million Identity Theft Insurance**

Enrollment Instructions

To enroll in Identity Defense, visit app.identitydefense.com/enrollment/activate/centralresources

1. **Enter your unique Activation Code** <<Activation Code>>
   Enter your Activation Code and click 'Redeem Code'.
2. **Create Your Account**
   Enter your email address, create your password, and click 'Create Account'.
3. **Register**
   Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. **Complete Activation**
   Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Enrollment Deadline>>. After <<Enrollment Deadline>>, the enrollment process will close, and your Identity Defense code will no longer be active. **If you do not enroll by <<Enrollment Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.**

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 1.866.622.9303.

*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.