AT THE FOREFRONT
UChicago Medicine

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

## NOTICE OF DATA BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

At the University of Chicago Medical Center (UCMC), we are committed to protecting the confidentiality and security of your personal information. We are sending you this letter to let you know that UCMC was recently the victim of an email security incident that may have resulted in unauthorized access to your personal information. *At this time, we are not aware of any misuse of your personal information*.

## WHAT HAPPENED?

From March 24, 2022 to March 31, 2022, an unauthorized individual gained access to the email accounts of several UCMC employees. Upon learning of this incident on March 24, 2022, we took steps to terminate the unauthorized access, and secure the affected email accounts. We also promptly began an investigation into the incident with assistance from a leading cybersecurity provider and performed an analysis of the impacted email accounts.

We are notifying you of this incident because your personal information was available in at least one of the affected email accounts.

## WHAT INFORMATION WAS INVOLVED?

The affected UCMC employees' email accounts contained the following types of personal information, some of which may have been included about you: first and last name; Social Security number; health information, such as diagnoses and prescriptions; legacy Medicare beneficiary identification number that includes Social Security number; health insurance policy number, and driver's license number. UCMC may have previously collected your information because you or a family member were a patient or otherwise received services from us.

## WHAT WE ARE DOING

We have implemented additional security measures to prevent the occurrence of a similar event in the future. For example, we have enhanced our user authentication controls and our threat monitoring and detection processes.We are also providing ongoing training to our employees on the importance of email security.

Although we have no reason to believe that your information has been, or will be, misused because of this incident, we would like to offer you two years of free identity monitoring services from Kroll. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

*You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.*

Membership Number: **<<Membership Number s_n>>**

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

In addition to enrolling in Kroll's identity monitoring services, you should consider taking the following steps to protect yourself:

- Read account statements from your health care providers, explanations of benefits (EOBs) from your health plan and other documents related to medical services to make sure they do not include services you did not receive.
- Be attentive to documents related to medical services that you usually receive and that suddenly do not arrive, as you usually receive them.
- All mail related to medical or financial information should be destroyed and preferably shredded before you throw it away.
- Be careful when offering personal information over the phone, mail or internet, and unless you are sure of the person with whom you are dealing, offer as little information as possible.
- Review the "General Information About Identity Theft Protection" materials that are included with this letter. You should always remain vigilant for threats of fraud and identity theft by regularly reviewing your account statements and credit reports.

## FOR MORE INFORMATION

We regret this incident and apologize for any inconvenience it may cause you. If you have any questions or concerns, please call (855) 503-2963, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding some major U.S. holidays.

Sincerely,

Karen Habercoss
Chief Privacy Officer
The University of Chicago Medicine

## GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

**Credit Reports.** Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. **You may contact the nationwide credit reporting agencies at:**

| **Equifax** | **Experian** | **TransUnion** |
|---|---|---|
| P.O. Box 105788 Atlanta, GA 30348 | P.O. Box 9554 Allen, TX 75013 | P.O. Box 2000 Chester, PA 19016 |
| www.equifax.com | www.experian.com | www.transunion.com |
| (800) 525-6285 | (888) 397-3742 | (800) 680-7289 |

**Fraud Alert.** You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

**Place a Security Freeze on your Credit Report.** You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed at above. 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 be able to use an online process, an automated telephone line or a written request. 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 five 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. You can place a freeze and lift a security freeze on your credit report free of charge.

**You may contact the Federal Trade Commission (FTC) 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 contact the FTC and/or your state's attorney general office about for information on how to prevent or avoid identity theft. You can contact the FTC at: **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

**For District of Columbia Residents:** District of Columbia Office of the Attorney General, 400 6th St. NW, Washington, DC 20001, https://oag.dc.gov, (202) 727-3400

**For Iowa Residents:** State law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590

**For Maryland Residents:** 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 New Mexico Residents:** You have certain rights pursuant to the federal Fair Credit Reporting Act (FCRA). For more information about the FCRA, please visit www.ftc.gov

**For North Carolina Residents:** North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, 1-877-566-7226.

KROLL

## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

**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.

**Web Watcher**

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

**Public Persona**

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

**Quick Cash Scan**

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

**$1 Million Identity Fraud Loss Reimbursement**

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

**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.