



Return Mail Processing  
PO Box 999  
Suwanee, GA 30024

35 1 10283 \*\*\*\*\*SNGLP

SAMPLE A. SAMPLE - L01



APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



May 24, 2024

### NOTICE OF DATA BREACH

Dear Sample A. Sample,

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 January 4, 2024 to January 30, 2024, an unauthorized individual gained access to the email accounts of a small number of UCMC workers. Upon learning of this incident, 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. On March 28, 2024, we determined that your personal information was available in at least one of the affected email accounts.

#### WHAT INFORMATION WAS INVOLVED?

The affected UCMC workers' email accounts contained the following types of personal information, some of which may have been included about you: first and last name; date of birth; Social Security number; tax identification number; IRS PIN number; passport number; driver's license or state issued identification number; military identification number; non-U.S. national identification number; account number; routing number; financial institution name; credit or debit card number and security code or PIN; access information, such as access credentials, security questions and answers, and digital signatures; health information, such as information about diagnoses and treatment, prescriptions, provider name, medical record number or patient identification number, or hospital account record number; health insurance information, such as Medicare or Medicaid number or health insurance subscriber number. UCMC may have previously collected your information because you were, or a family member of yours was, 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, early alert capabilities, 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 are offering a complimentary 24-month membership of Experian's® IdentityWorks<sup>SM</sup>. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: August 30, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-918-4065 by **August 30, 2024**. Be

prepared to provide engagement number B123131 as proof of eligibility for the identity restoration services by Experian.

### **WHAT YOU CAN DO**

In addition to enrolling in Experian'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 if you receive unexpected communications related to medical services, if you no longer receive expected communications from us, or if communications seeming to come from us arrive through an unexpected way of communication.
- Before you throw away any mail containing medical or financial information, you should shred it or destroy it in another way that renders it unreadable.
- 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 833-918-4065 toll-free, Monday through Friday from 8am to 8pm Central Time, excluding some major U.S. holidays. Be prepared to provide your engagement number B123131.

Sincerely,

Karen Habercoss  
Chief Privacy Officer  
The University of Chicago Medical Center

## 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](http://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](http://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 <a href="http://www.equifax.com">www.equifax.com</a> (800) 525-6285	P.O. Box 9554 Allen, TX 75013 <a href="http://www.experian.com">www.experian.com</a> (888) 397-3742	P.O. Box 2000 Chester, PA 19016 <a href="http://www.transunion.com">www.transunion.com</a> (800) 916-8800

**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.

**Credit Freezes (for Non-Massachusetts and Non-Iowa Residents):** You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as indicated above.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

**Credit Freezes (for Massachusetts Residents):** Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the respective address indicated above.

**Credit Freezes (for Iowa Residents):** Iowa law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the respective address indicated above.

*Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report.

**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](http://www.ftc.gov), 1-877-IDTHEFT (438-4338).

**If you are a Connecticut resident**, you may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, [www.ct.gov/ag](http://www.ct.gov/ag).

**If you are a District of Columbia resident**, you may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001, 1-202-727- 3400, [www.oag.dc.gov](http://www.oag.dc.gov).

**If you are an Iowa resident**, 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.

**If you are a Kentucky resident**, you can obtain information about steps you may take to avoid identity theft from following sources: the FTC (see contact information above), the major consumer credit reporting agencies (see contact information above), and the Office of the Kentucky Attorney General: 700 Capital Avenue, Suite 118, Frankfort, KY 40601-3449, [www.ag.ky.gov](http://www.ag.ky.gov), 1-888- 432-9257.

**If you are a Maryland resident**, you can contact the Maryland Office of the Attorney General, Consumer Protection Division at: 200 St. Paul Place, Baltimore, MD 21202, [www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov), 1-888-743-0023.

**If you are a Massachusetts resident**, under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, [www.mass.gov/contact-the-attorney-generals-office](http://www.mass.gov/contact-the-attorney-generals-office).

**If you are a New Mexico resident**, you have certain rights pursuant to the federal Fair Credit Reporting Act (FCRA). For more information about the FCRA, please visit [www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act](http://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act) or [www.ftc.gov](http://www.ftc.gov).

**If you are a New York resident**, you can contact the New York Office of the Attorney General at [www.ag.ny.gov](http://www.ag.ny.gov), 1- 800-771-7755; the New York Department of State, [www.dos.ny.gov](http://www.dos.ny.gov), 1-800-697-1220; and the New York Division of State Police, [www.ny.gov/agencies/division-state-police](http://www.ny.gov/agencies/division-state-police), (914) 834-9111.

**If you are a North Carolina resident**, you can contact the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, <https://ncdoj.gov>, 1-877-566-7226.

**If you are an Oregon resident**, state law advises you to report any suspected identity theft to law enforcement or to the FTC.

**If you are a Rhode Island resident**, you have the right to obtain a police report. You also have the right to request a security freeze, as described above. You can also contact the Office of the Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, [www.riag.ri.gov](http://www.riag.ri.gov), (401) 274-4400 or file a police report by contacting (401) 444-1000.

**If you are a West Virginia resident**, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.



Return Mail Processing  
PO Box 999  
Suwanee, GA 30024

35 1 10328 \*\*\*\*\*SNGLP

SAMPLE A. SAMPLE - L02

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



May 24, 2024

### NOTICE OF DATA BREACH

Dear Sample A. Sample,

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 January 4, 2024 to January 30, 2024, an unauthorized individual gained access to the email accounts of a small number of UCMC workers. Upon learning of this incident, 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. On March 28, 2024, we determined that your personal information was available in at least one of the affected email accounts.

#### WHAT INFORMATION WAS INVOLVED?

The affected UCMC workers' email accounts contained the following types of personal information, some of which may have been included about you: first and last name; date of birth; health information, such as information about diagnoses and treatment, prescriptions, provider name, medical record number or patient identification number, hospital account record number; health insurance policy number; or treatment cost. UCMC may have previously collected your information because you or a family member was 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, early alert capabilities, and our threat monitoring and detection processes. We are also providing ongoing training to our employees on the importance of email security.

#### WHAT YOU CAN DO

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 if you receive unexpected communications related to medical services, if you no longer receive expected communications from us, or if communications seeming to come from us arrive through an unexpected way of communication.
- Before you throw away any mail containing medical or financial information, you should shred it or destroy it in another way that renders it unreadable.
- 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 833-918-4065 toll-free, Monday through Friday from 8am to 8pm Central Time, excluding some major U.S. holidays. Be prepared to provide your engagement number B123133.

Sincerely,

Karen Habercoss  
Chief Privacy Officer  
The University of Chicago Medical Center

## 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](http://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](http://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 <a href="http://www.equifax.com">www.equifax.com</a> (800) 525-6285	P.O. Box 9554 Allen, TX 75013 <a href="http://www.experian.com">www.experian.com</a> (888) 397-3742	P.O. Box 2000 Chester, PA 19016 <a href="http://www.transunion.com">www.transunion.com</a> (800) 916-8800

**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.

**Credit Freezes (for Non-Massachusetts and Non-Iowa Residents):** You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as indicated above.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

**Credit Freezes (for Massachusetts Residents):** Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the respective address indicated above.

**Credit Freezes (for Iowa Residents):** Iowa law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the respective address indicated above.

*Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report.

**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](http://www.ftc.gov), 1-877-IDTHEFT (438-4338).

**If you are a Connecticut resident**, you may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, [www.ct.gov/ag](http://www.ct.gov/ag).

**If you are a District of Columbia resident**, you may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001, 1-202-727- 3400, [www.oag.dc.gov](http://www.oag.dc.gov).

**If you are an Iowa resident**, 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.

**If you are a Kentucky resident**, you can obtain information about steps you may take to avoid identity theft from following sources: the FTC (see contact information above), the major consumer credit reporting agencies (see contact information above), and the Office of the Kentucky Attorney General: 700 Capital Avenue, Suite 118, Frankfort, KY 40601-3449, [www.ag.ky.gov](http://www.ag.ky.gov), 1-888- 432-9257.

**If you are a Maryland resident**, you can contact the Maryland Office of the Attorney General, Consumer Protection Division at: 200 St. Paul Place, Baltimore, MD 21202, [www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov), 1-888-743-0023.

**If you are a Massachusetts resident**, under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, [www.mass.gov/contact-the-attorney-generals-office](http://www.mass.gov/contact-the-attorney-generals-office).

**If you are a New Mexico resident**, you have certain rights pursuant to the federal Fair Credit Reporting Act (FCRA). For more information about the FCRA, please visit [www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act](http://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act) or [www.ftc.gov](http://www.ftc.gov).

**If you are a New York resident**, you can contact the New York Office of the Attorney General at [www.ag.ny.gov](http://www.ag.ny.gov), 1- 800-771-7755; the New York Department of State, [www.dos.ny.gov](http://www.dos.ny.gov), 1-800-697-1220; and the New York Division of State Police, [www.ny.gov/agencies/division-state-police](http://www.ny.gov/agencies/division-state-police), (914) 834-9111.

**If you are a North Carolina resident**, you can contact the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, <https://ncdoj.gov>, 1-877-566-7226.

**If you are an Oregon resident**, state law advises you to report any suspected identity theft to law enforcement or to the FTC.

**If you are a Rhode Island resident**, you have the right to obtain a police report. You also have the right to request a security freeze, as described above. You can also contact the Office of the Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, [www.riag.ri.gov](http://www.riag.ri.gov), (401) 274-4400 or file a police report by contacting (401) 444-1000.

**If you are a West Virginia resident**, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.