

[LOGO]

Return Processing Center

<<Return Address>>

To Enroll, Please Visit:
[https://app.idx.us/account-
creation/protect](https://app.idx.us/account-creation/protect)
Enrollment Code: [Code]

29881

Address Block

<<Date>>

Dear Name:

We are writing to inform you of a data security incident experienced by University of Health Sciences & Pharmacy (“UHSP”) that may have involved your information as described below. We take the privacy and security of all information very seriously, and while we have no evidence to suggest that any information was subject to actual or attempted misuse as a result of this incident, we are notifying potentially impacted individuals out of an abundance of caution. This letter includes information about the incident, our response, and steps you can take to help protect your information should you feel it appropriate to do so.

What Happened: On April 13, 2023, we received an alert of a potential hardware failure. Upon notification, UHSP’s IT Department began an internal investigation and restored affected systems as quickly as possible. On April 20, 2023, UHSP experienced a second suspected hardware failure which prompted an immediate investigation with the assistance of leading, independent cybersecurity specialists to determine the full nature and scope of this incident. Based on this investigation, we have discovered that certain folders were subject to unauthorized access as part of this incident and are notifying individuals whose information was potentially impacted in an abundance of caution.

What Information Was Involved: The information at risk of unauthorized access includes information stored within your UHSP network drive and may include, among other things, your first and last name in combination with one or more of the following data elements: Social Security Number.

What We Are Doing: We have taken the steps necessary to address the incident and are committed to protecting all of the information that you have entrusted to us. Upon learning of this incident, we immediately took steps to secure our systems and to enhance the security of our network. Out of an abundance of caution, we have also arranged for you to activate, at no cost to you, an online credit monitoring service for 12 months provided by IDX. Due to privacy laws, we cannot activate these services for you directly. Additional information regarding how to activate the complimentary credit monitoring service is enclosed.

What You Can Do: We recommend that you remain vigilant against incidents of fraud and identity theft by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. You can also review the enclosed “Steps You Can Take to Help Protect Your Information” for additional resources.

For More Information: Should you have additional questions or concerns regarding this matter, please do not hesitate to contact us at [number]. You can also write to us at 1 Pharmacy Place, St. Louis, MO 63110.

We stay committed to protecting your trust in us and continue to be thankful for your support.

Sincerely,

David Allen
President

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring Services

1. **Website and Enrollment.** Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
2. **Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
3. **Telephone.** Contact IDX at 1-800-939-4170 to speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

ADDITIONAL ACTIONS TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); 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.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file/obtain a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.