



THE COLLEGE OF
HEALTH CARE PROFESSIONS

For the Career of Your Life

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

March 26, 2021

G3343-L01-0000001 T00001 P001 *****AUTO**MIXED AADC 159

SAMPLE A. SAMPLE - L01 STANDARD

APT ABC

123 ANY ST

ANYTOWN, ST 12345-6789



Re: Notice of Data [EXTRA1]

Dear Sample A. Sample:

The College of Health Care Professions (“CHCP”) is writing to notify you of an incident that may affect the privacy of some of your personal information. While we are unaware of any actual or attempted misuse of your information, we take this incident very seriously. This letter provides details of the incident and the resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

What Happened? On September 21, 2020, CHCP became aware of suspicious activity relating to an employee email account that was sending unauthorized messages. We immediately launched an investigation to determine what may have happened. We determined that an unauthorized individual accessed two employee email accounts between approximately March 5, 2020 and October 3, 2020. Because we were unable to determine which email messages in the two accounts may have been viewed by the unauthorized actor, we reviewed the entire contents of the affected email accounts to identify what personal information was accessible to the unauthorized actor. After a thorough review, CHCP identified the impacted individuals on February 10, 2021. Once we identified the individuals who were potentially impacted, CHCP worked to confirm current mailing addresses for the impacted individuals and prepare an accurate written notice of this incident.

What Information Was Affected? Although we cannot confirm whether your personal information was actually accessed or viewed without permission, we are providing you this notification out of an abundance of caution, because such activity cannot be ruled out. The following types of your information were present in an email or attachment that was located in one of the affected email accounts at the time of the unauthorized access and may have been viewed by an unauthorized actor: your name and [EXTRA2].

What Are We Doing? CHCP has strict security measures to protect the information in our possession. Upon learning of this incident, we changed the affected employees’ email account passwords and took steps to secure the accounts. We are currently implementing extensive additional technical safeguards on our email system and providing additional training and education for employees to help prevent similar future incidents.

What Can You Do? Although we are unaware of any fraudulent misuse of your information, we have arranged to have Experian provide complimentary credit monitoring to you for [EXTRA3] months as an added precaution. Please review the instructions contained in the enclosed “Steps You Can Take to Protect Your Information” to enroll in and receive these services. CHCP will cover the cost of this service; however, you will need to enroll yourself in the credit monitoring service.

0000001



For More Information: We recognize that you may have questions not addressed in this letter. If you have additional questions, please contact our dedicated assistance line at (866) 274-4371, Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central, excluding major U.S. holidays. Be prepared to provide your engagement number DB26131. You may also write to us at 2550 North Loop W., Houston, TX 77092.

We sincerely regret any inconvenience this incident may cause you. CHCP remains committed to safeguarding the information in our care and we will continue to take steps to ensure the security of our systems.

Sincerely,

Bill Kohlhoff

Bill Kohlhoff
Senior Vice President of Accreditation, Chief Compliance Officer
The College of Health Care Professions

Steps You Can Take to Protect Your Information

Enroll in Credit Monitoring.

To help protect your identity, we are offering a complimentary [EXTRA3]-month membership of Experian's® IdentityWorksSM. 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: June 30, 2021** (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 **(866) 274-4371** by **June 30, 2021**. Be prepared to provide engagement number **DB26131** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [EXTRA3]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (866) 274-4371. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

0000001



Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, 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, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer’s 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 to take control over who gets access to the personal and financial information in your credit report 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 security freeze, you will need to provide the following information:

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

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file 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 and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 441 4th St. NW #1100 Washington, D.C. 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. CHCP is located at 2550 North Loop W., Houston, TX 77092.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For 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 bureaus 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 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. We encourage you to 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.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

