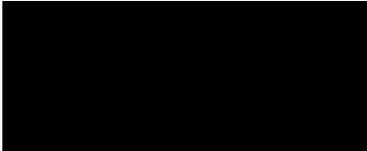


Graham Hospital Association
Mail Handling Services
777 E Park Dr
Harrisburg, PA 17111



October 2, 2020



C-433

Dear



Graham Hospital Association (“Graham Hospital”) is committed to protecting the privacy and confidentiality of personal information. This is why we are writing to inform you of a recent incident that may have exposed some of your personal information to an unintended audience.

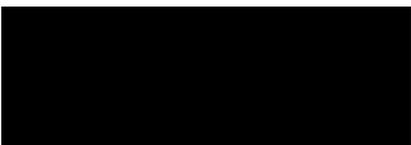
We recently learned that the PaperlessPay Corporation (“PaperlessPay”) experienced a data security incident. PaperlessPay is the vendor that we contract with for the provision of online bi-weekly paystubs and W-2 tax forms. According to PaperlessPay, on February 19, 2020, the Department of Homeland Security (“DHS”) contacted PaperlessPay and notified it that someone was purporting to sell access to the PaperlessPay client database on the dark web. In response, PaperlessPay shut down its web server and SQL server to prevent unauthorized access. It then worked with the FBI and retained a cybersecurity firm to conduct a forensic investigation. That investigation revealed that someone accessed PaperlessPay’s SQL server on February 18, 2020. PaperlessPay recently provided Graham Hospital a list of data elements which might have been compromised as a result of the data security incident. **We understand that there is no evidence that the incident resulted in the unauthorized acquisition of any of our employees’ personal information**, but PaperlessPay could not definitively rule out the possibility that someone viewed or acquired our employees’ information; therefore, we are providing this notification and have arranged for complimentary identity theft protection services for potentially impacted employees.

On or around August 11, 2020, our investigation determined that the potentially impacted PaperlessPay server holds paystubs and W-2 tax forms that contain personal information, including your name, address, pay and withholdings, and Social Security number.

At this point, we do not know for certain if any of your personal information was acquired by an unauthorized party, and we are not aware of any instances of fraud or identity theft resulting from this incident. We have arranged for a complimentary one-year membership of Experian IdentityWorksSM Credit 3B for all potentially impacted employees. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. Experian IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. **For more information on Experian IdentityWorks Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**

We take our responsibility to safeguard personal information seriously and apologize for any inconvenience or concern this incident might cause. For further information and assistance, please call [REDACTED] Monday through Friday, 8:00 AM CST- 5:00 PM CST.

Sincerely,



To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: [REDACTED] (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **Activation Code**: [REDACTED]

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 877-288-8057. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **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, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at <https://www.experianidworks.com/3bcredit> or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

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

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps to you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC – Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting <http://www.annualcreditreport.com>, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files, is as follows:

Equifax 1-800-349-9960 www.equifax.com P.O. Box 105788 Atlanta, GA 30348	Experian 1-888-397-3742 www.experian.com P.O. Box 9554 Allen, TX 75013	TransUnion 1-888-909-8872 www.transunion.com P.O. Box 2000 Chester, PA 19022
---	--	--

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at <http://www.annualcreditreport.com>.

Credit and Security Freezes: You may have the right to place 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 the 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 using the contact information above.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfc_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.