PARKVIEW
HEALTH

[redacted]

[redacted]

[redacted]

Dear [redacted]:

Parkview Health is committed to maintaining the privacy of its co-workers and takes protecting personal information seriously. This is why we are writing to inform you of an incident that may have exposed some of your personal information to an unintended audience. PaperlessPay Corporation ("PaperlessPay"), the vendor who previously provided Parkview co-workers with access to online bi-weekly paystubs and W-2 tax forms, informed Parkview that it experienced a data security incident. On September 2, 2020, our investigation determined that the potentially impacted PaperlessPay server holds W-2 tax forms and paystubs that contain personal information, including your name, address, pay and withholdings, and Social Security number.

Our understanding is that there is no evidence that the incident resulted in the unauthorized acquisition of any of our co-workers' personal information, and we are not aware of any instances of fraud or identity theft arising out of this situation. PaperlessPay, however, could not definitively rule out the possibility that someone viewed or could have acquired our co-workers' information. Therefore, out of caution, we are providing this notification to potentially impacted co-workers.

We have also arranged for a complimentary one-year membership of Experian IdentityWorks^{SM} Credit 3B for potentially impacted co-workers. 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 with this letter.**

We take our responsibility to safeguard personal information seriously and apologize for this inconvenience and concern this incident might cause. For further information and assistance, Parkview has established an information line to serve co-workers during this time. Please call [redacted] or [redacted], Monday through Friday, 9:00 AM EST to 5:00 PM EST to speak with an individual who will be able the further assist in answering your questions.

Sincerely,

[redacted]

0000004

F8774-L04

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks℠ 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 877-890-9332. 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 ExtendCARE™**: 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 877-890-9332 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 877-890-9332.

* 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.*

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	Experian	TransUnion
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	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 as specified below to find out more information:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

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/bcfp_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.

For residents of the following states:

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, http://www.marylandattorneygeneral.gov/.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; https://ag.ny.gov/consumer-frauds/identity-theft; (800) 771-7755.

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.

Frequently Asked Questions

Q. What happened?
A. Earlier this year, the PaperlessPay Corporation, the vendor Parkview previously used to provide co-workers with online bi-weekly paystubs and W-2 tax forms, experienced a security incident. According to PaperlessPay, the Department of Homeland Security notified PaperlessPay that someone attempted to sell access to PaperlessPay's client database on the dark web. PaperlessPay retained a cybersecurity firm to conduct a forensic investigation. The investigation revealed that an unauthorized user accessed PaperlessPay's server on February 18, 2020.

Q. Who did this?
A. We do not know the identity of the individual or individuals responsible for this incident.

Q. Why am I receiving this letter?
A. Parkview is notifying you out of an abundance of caution because your personal information, including social security number, was contained within the impacted PaperlessPay database. Parkview does not know for certain if your information was ever viewed or acquired by the unauthorized third party and is not aware of any instances of fraud or identity theft as a result of this incident. However, Parkview takes the privacy and confidentiality of your information seriously, which is why we notified you to provide you with information about this incident and steps you can take to protect yourself as a precaution should you choose to do so.

Q. What specific information of mine was affected?
A. As part of its investigation, Parkview learned that the compromised PaperlessPay database contained Parkview co-workers' bi-weekly paystubs and W-2 tax forms. The information that could have been viewed includes the information on your Parkview paystubs and the information on your 2015-2019 W2 tax forms.

Q. Do you suspect that my information has been used fraudulently? Has anyone been adversely affected as a result of this incident?
A. There is no evidence to suggest that your or anyone else's information has been misused in any way and we are not aware of any instances of fraud or identity theft resulting from this incident. At this point, we do not even know for certain if any of your personal information was acquired by an unauthorized party. That said, we recommend you review the information in the notification letter on steps you can take to protect yourself from fraud if you have concerns.

Q. How will I know if my information was used by someone else?
A. The Federal Trade Commission has published tips for people on protecting their identity. These tips include warning signs of identity theft and can be found on the FTC website at www.ftc.gov/idtheft. See above for additional information.