Notice of Data Breach

This notice concerns a recent incident involving United Bank, a financial institution that provides certain payment processing services for Camden-Clark Physician Corporation and Camden-Clark Memorial Hospital Corporation (collectively "Camden-Clark"). United Bank takes the confidentiality of personal information of Camden-Clark's patients very seriously.

Please note: This notice explains an incident that has been determined to have affected ***individuals who made a payment, or on whose behalf a payment was made, by check or money order to Camden-Clark between December 1, 2022 and May 30, 2023***. For these individuals, this notice explains the complimentary services United Bank has arranged to support you, and other steps you may wish to take to protect your personal information.

What Happened:

United Bank informed Camden-Clark of the compromise of MOVEit, a third-party software tool used by hundreds of companies around the world, including United Bank, to assist in the secure transfer of files. The compromise was disclosed by MOVEit's manufacturer, Progress Software, and has been widely reported in the media to have affected a large number of companies.

What Information Was Involved:

United Bank has conducted an investigation of the incident with the assistance of third party experts. As a result of its investigation, it has determined that on approximately May 30, 2023, an unauthorized third party obtained files that included certain personal information of ***individuals who made a payment, or on whose behalf a payment was made, by check or money order to Camden-Clark between December 1, 2022 and May 30, 2023***.

The information varied by individual but may have included one or more of the following: name, address, date of birth, telephone number, social security number, driver's license number, payment account number, health insurance identifying number, financial information and/or medical or treatment-related information found on records of payment or explanation of benefits statements.

What We Are Doing:

Upon learning of the incident, United Bank immediately took measures to mitigate the impact. It took its MOVEit server offline and promptly applied all recommended remediation measures. It also launched the investigation described above, which has now concluded. The incident did not involve any passwords related to bank accounts.

On June 13, 2023, United Bank informed Camden-Clark of the incident, and has worked since that time with external advisers to determine which individuals and data were affected. MOVEit software did not run on United Bank's core systems, which it has confirmed were unaffected by the incident.

This notice contains additional information concerning steps individuals who may have been affected by this incident can take to monitor and protect their personal information. In addition, United Bank will make available complimentary credit monitoring through Equifax for affected individuals. ***Individuals who made a payment, or on whose behalf a payment was made, by check or money order to Camden-Clark between December 1, 2022 and May 30, 2023*** **may call (888) 988-0348** on weekdays between the hours of 9 AM – 9 PM EST for additional information.

What You Can Do:

Affected individuals should remain vigilant for the next 24 months for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, report it immediately to your financial institutions.

In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement, including your state Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's website at www.ftc.gov/idtheft, call the FTC at (877) IDTHEFT (438-4338), or write to the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580.

You may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under the federal Fair Credit Reporting Act ("FCRA"), 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 or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax	**Experian**	**TransUnion**
(800) 685-1111	(888) 397-3742	(888) 909-8872
P.O. Box 740256	P.O. Box 9554	TransUnion Fraud Victim
Atlanta, GA 30374-0241	Allen, TX 75013	Assistance Department
www.Equifax.com/personal/	www.Experian.com/help	P.O. Box 2000
credit-report-services		Chester, PA 19016
		www.TransUnion.com/credit-help

You also have other rights under the FCRA. For further information, please visit: https://files.ConsumerFinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.docx (English) or https://files.ConsumerFinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09_es.docx (Spanish).

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult

for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. In addition, you can contact the nationwide credit reporting agencies at the following numbers to place a security freeze to restrict access to your credit report:

1. Equifax – (800) 685-1111
2. Experian – (888) 397-3742
3. TransUnion – (888) 909-8872

You will need to supply your name, address, date of birth, Social Security number, and other personal information. After receiving your request, each credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need in order to lift or remove the freeze. You should keep the PIN or password in a safe place.

For More Information:

Individuals with questions related to this incident may call the toll-free designated call center at (**888) 988-0348** on weekdays between the hours of 9 AM – 9 PM EST.