TBK BANK

30868

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Dear <<First_Name>> <<Last_Name>>,

We are writing to inform you of a security incident involving software utilized by one of our third party service providers through which some of your personal information was disclosed to an unknown and unauthorized third party. Because TBK Bank takes the security and privacy of your personal information very seriously, we are sending you this notice to explain what happened, what information was involved, what measures we and our third party service provider are taking in response, and what steps you can take to protect yourself.

What Happened?

On August 8, 2023, TBK Bank was notified by Fiserv, our third party service provider, that certain TBK Bank customer data processed by them had been involved in a security incident. Upon being notified, TBK Bank immediately launched an investigation into the incident. We also started working to identify which TBK Bank customers may have had their information impacted by the incident.

As we have learned from our service provider, the security incident resulted from the exploitation of a vulnerability in the MOVEit Transfer software. MOVEit Transfer, which Progress Software owns, is a file transfer software used by our service provider to support its services to TBK Bank. According to their analysis, the incident took place between May 27, 2023, and May 31, 2023, prior to the public disclosure of the MOVEit vulnerability by Progress Software. During that time, an unknown and unauthorized third party obtained files transferred by the service provider via the MOVEit Transfer software. Based on our investigation, we learned that certain files the unauthorized third party acquired contained your personal information (as described below). Upon this discovery, we worked diligently with our service provider to notify you of the data breach.

What Information Was Involved?

TBK Bank and Fiserv have conducted a careful review of the contents of the files acquired by the unauthorized third party and have determined that one or more of the files contained the following pieces of your personal information: <<b2b_text_3 (your name, impacted data elements)>>.

What We Are Doing.

While this event did not affect TBK Bank systems, networks or business operations, we take data privacy and security very seriously and expect the same from our vendors. TBK Bank took immediate steps to launch a comprehensive investigation after we were notified of the MOVEit incident. We worked to understand what happened, who was impacted, and what steps were taken to remediate this incident and prevent future incidents like this from occurring.

In response to the incident, Fiserv took immediate steps to disable the unauthorized access to Progress Software's MOVEit Transfer system and to patch the MOVEit environment to remediate the vulnerabilities according to Progress Software's security guidance. They also mobilized a technical response team of third party forensic experts to examine the relevant MOVEit Transfer systems and ensure that there were no further vulnerabilities. They have also contacted law enforcement.

Though there is no evidence to suggest that your personal information has been fraudulently used, out of an abundance of caution, we are offering you 24 months of free fraud detection and identity theft protection through Kroll. If you wish to take advantage of these services, activation instructions are below.

What You Can Do.

Though there is no evidence that your personal information has been published to any unauthorized websites or otherwise misused or disclosed, we encourage you to remain vigilant by reviewing your account statements and credit reports closely. In Attachment B, we have provided you with additional information regarding steps you can proactively take to protect yourself and your personal information further. It describes information about (1) reporting suspicious activity or suspected identity theft, (2) credit reports, (3) fraud alerts, (4) credit/security freezes, and (5) your rights under the Fair Credit Reporting Act. We encourage you to review that additional information.

We have arranged for you to receive a free identity monitoring service through Kroll for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained unintentional exposure of confidential data. Your identity monitoring services include credit monitoring, fraud consultation and identity theft restoration.

For more information and instructions on activating your identity monitoring, please review Attachment A to this letter.

For More Information.

While the MOVEit security event has impacted many organizations globally, TBK Bank remains focused on protecting your personal information. Please be assured that we are taking steps to address the incident with our service provider and to help protect the security of your data. If you have any questions about this notice or the incident, please feel free to contact our call center to address questions about this incident at 800-768-4880, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Thank you,

Todd Ritterbusch
President
TBK Bank, SSB

ATTACHMENT A

Free credit monitoring and identification theft protection instructions

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (Activation Deadline)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number (S_N)>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

KROLL

You have been provided with access to the following services from Kroll for two years. This coverage will not automatically renew at the end of the two years.

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to help protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ATTACHMENT B

Additional steps you can take to protect your personal information

To help protect against possible fraud, identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements and to monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report, and place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft you should consider contacting your local law enforcement agency, filing a police report, or contacting your state's Attorney General or the Federal Trade Commission.

Information on Obtaining a Free Credit Report: U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

Information on Implementing A Fraud Alert, Credit Freeze, or Credit Lock: To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three consumer reporting agencies below:

Equifax:	Experian:	TransUnion:
Equifax Information Services LLC	Credit Fraud Center	Fraud Victim Assistance Department
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-888-298-0045	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Fraud Alert: Consider contacting the three major consumer reporting agencies at the addresses above to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you

credit. Although this may cause some short delay if you are the one applying for the credit, it might help protect against someone else obtaining credit in your name.

To place a fraud alert, contact any of the three major consumer reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts 90 days but can be renewed.

Credit Freeze: A credit freeze prohibits a consumer reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. When a credit freeze is in place, no one—including you—can open a new account. As a result, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services.

Placing a credit freeze is free. To place a credit freeze, contact all three consumer reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior 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. If you are a victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

When you place a credit freeze, you will be provided a PIN to lift temporarily or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven years.

Credit Lock: Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three consumer reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charges monthly fees.

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, credit freezes, credit locks, and how to help protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone 1-877-IDTHEFT; or www.consumer.gov/idtheft. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a compliant by way of the contact information listed above.

ADDITIONAL RESOURCES

Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, or the FTC.

District of Columbia Residents: The Attorney General can be contacted at the Office of the Attorney General, 441 4th Street NW, Washington, DC 20001; (202) 727-3400; or https://oag.dc.gov/.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or http://www.oag.state.md.us.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; or http://www.ncdoj.gov.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

Rhode Island Residents: The Attorney General can be contacted at (401) 274-4400 or http://www.riag.ri.gov/. You may also file a police report by contacting local or state law enforcement agencies.