



<<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 INCIDENT

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Kirkwood Bank & Trust values and respects your privacy, which is why we are writing to advise you of a recent incident that occurred at one of our vendors that may have involved some of your personal information. **At this time, we do not have any evidence that your personal information has been misused as a result of this incident.** Nonetheless, out of an abundance of caution, we are notifying you about the incident and the steps taken to address it. This letter also describes steps you may take to help protect your information, should you feel it is appropriate to do so.

What Happened?

MOVEit Transfer is a commonly used Managed File Transfer software used by government agencies, corporations, financial institutions, and other organizations worldwide. Kirkwood Bank & Trust does not directly use MOVEit. However, Fiserv, a third-party vendor Kirkwood Bank & Trust uses as our core processor, experienced an incident involving the MOVEit Transfer application, provided by Progress Software. Upon discovering the incident, our vendor promptly launched an investigation into the nature and scope of the incident's impact on its systems. Our vendor's investigation determined that an unauthorized third party exploited a previously unknown vulnerability in MOVEit that allowed the third party to gain access to files to the vendor's MOVEit Transfer application between May 27 and 31, 2023. This timeframe was before the existence of this vulnerability was publicly disclosed. During that time, unauthorized actors obtained certain files transferred via MOVEit. These files contained certain Kirkwood Bank & Trust customer information, including yours. We were recently notified by our vendor and immediately activated our Incident Response Program.

Importantly, the incident did not involve unauthorized access to any of Kirkwood Bank & Trust's internal systems and did not impact our ability to service our customers.

What Information Was Involved?

Our vendor conducted a careful review of the contents of the files and determined that one or more of the files acquired by the third party may have contained information including your name, business name, dates of birth, address, state, telephone number, account number, routing number, social security numbers and other tax IDs.

What We Are Doing.

We wanted to notify you of this incident and to assure you that we take it seriously. Upon learning of this incident, Kirkwood Bank took immediate action to ensure that our vendor had launched a comprehensive investigation, identified individuals affected and notified regulatory bodies as required. To help prevent something like this from happening again our vendor has remediated all technical vulnerabilities and patched systems in accordance with the MOVEit software provider's guidelines. Our vendor has mobilized a technical response team to examine the relevant MOVEit systems to ensure that there were no further vulnerabilities.

What You Can Do.

We are partnering with Kroll Identity Monitoring to offer you 24 months of complimentary identity protection services. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation and Identity Theft Restoration.

For more information on identity prevention, including instructions on how to activate your identity monitoring, as well as some additional steps you can take for your protection, please review Attachments A and B that are enclosed with this letter.

Regardless of whether you elect to activate the identity monitoring service, we strongly recommend that you remain vigilant and regularly review and monitor all of your credit history to guard against any unauthorized transactions or activity. We also recommend that you closely monitor your account statement and notify us or any of your other financial institutions if you suspect any unauthorized activity.

For More Information.

Please be assured that we, along with our vendor, are taking steps to address the incident 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 vendor's dedicated response line at (866) 731-2928, Monday through Friday from 8:00 am to 5:30 pm Central Time, excluding major U.S. Holidays.

Sincerely,

Kirkwood Bank & Trust

ATTACHMENT A

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.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

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 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, 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:
Equifax Information Services LLC
P.O. Box 105788
Atlanta, GA 30348
1-888-298-0045
www.equifax.com

Experian:
Credit Fraud Center
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion:
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
1-800-680-7289
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 1-877-382-4357; or www.consumer.gov/idtheft.

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.

New York Residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Avenue, Albany, NY, 12231-001, (518) 474-8583/(800) 697-1220, <http://www.dos.ny.gov/consumerprotection>; and New York State Office of the Attorney General, The Capitol, Albany, NY, 12224-0341, (800) 771-7755, <https://ag.ny.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.