

July 19, 2023

**VIA EMAIL**

Attorney General Brenna Bird  
Office of the Attorney General  
Consumer Protection Division  
Security Breach Notifications  
1305 E Walnut Street  
Des Moines, IA 50319-0106  
Email: [consumer@ag.iowa.gov](mailto:consumer@ag.iowa.gov)

Re: Notice of Data Security Incident

Dear Attorney General Bird:

Constangy, Brooks, Smith & Prophete, LLP represents 1st Source Bank in connection with a recent data security incident described in greater detail below.

**1. What Happened**

On June 1, 2023, 1st Source Bank became aware of an alert issued by Progress Software – the company responsible for the MOVEit file transfer program – addressing a critical vulnerability affecting MOVEit, a solution used widely by businesses and government agencies, including 1st Source Bank, to securely transfer data. After becoming aware of the alert, 1st Source Bank took immediate steps to patch its MOVEit system in accordance with Progress Software’s instructions and conduct an internal assessment. 1st Source Bank thereafter engaged leading, independent cybersecurity experts to conduct a comprehensive investigation to determine the scope of potentially affected data. On June 24, 2023, 1st Source Bank learned that certain personal information belonging to its customers was contained within a file that may have been acquired without authorization in connection with the MOVEit software vulnerability. Since that time, 1st Source Bank has been collecting information needed to provide notice to potentially impacted individuals.

The information that may have been impacted in connection with this incident varied by individual but may have included individuals’ names, Social Security numbers, driver’s license or state identification card numbers, other government identification numbers, and/or dates of birth. Notably, 1st Source Bank is aware of no evidence indicating that potentially impacted information has been misused.

**2. Number of Iowa Residents Notified**

Between July 14, 2019 and July 19, 2019, 1st Source Bank notified five hundred thirteen (513) Iowa residents of this data security incident via U.S. First-Class Mail. A sample copy of the notification letter sent to potentially impacted individuals is included with this correspondence.

### **3. Steps Taken Relating to the Incident**

As soon as 1st Source Bank discovered the incident, 1st Source Bank took the steps described above. 1st Source Bank is also partnering with Kroll to provide access to complimentary identity monitoring services to notified individuals. Those services include Single Bureau Credit Monitoring, Web Watcher, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

### **4. Contact Information**

1st Source Bank remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me.

Best regards,

/s/ Alyssa R. Watzman

Alyssa R. Watzman  
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Enclosure: Sample Notification Letter



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

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country>>

<<b2b\_text\_1 (Subject: Notice of Data Breach or Security Incident)>>

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

I am writing to inform you of a recent data security incident that may have affected some of your personal information. 1st Source Bank is one of an estimated 2,500 organizations worldwide that may have recently been affected by the MOVEit software vulnerability. Please read this letter carefully as it contains information regarding the incident and steps you can take to help protect your personal information. We are here to help you.

**What Happened?** On June 1, 2023, we became aware of an alert issued by Progress Software – the company responsible for the MOVEit file transfer program – addressing a critical vulnerability affecting MOVEit, a solution used widely by businesses and government agencies, including 1st Source Bank, to securely transfer data. After becoming aware of the alert, we took immediate steps to patch our MOVEit system in accordance with Progress Software’s instructions and conduct an internal assessment. 1st Source thereafter engaged leading, independent cybersecurity experts to conduct a comprehensive investigation to determine the scope of potentially affected data. On June 24, 2023, we learned that your data was contained within a file that may have been acquired without authorization in connection with the MOVEit software vulnerability. Since that time, we have been collecting information needed to provide notice to potentially impacted individuals, including you.

**What Information Was Involved?** The information potentially impacted in connection with this incident may have included your name as well as your Social Security number, driver’s license or state identification card number, other government-issued identification number, and/or date of birth.

**What Are We Doing?** As soon as we discovered the incident, we took the steps described above. In addition, we are providing you with information about steps that you can take to help protect your personal information. Furthermore, to help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide complimentary Identity Monitoring services for 12 months. Kroll is a global leader in risk mitigation and response, and the Kroll team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your Identity Monitoring services include Credit Monitoring, Web Watcher, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

**What You Can Do:** 1st Source recommends that you review the guidance included with this letter about how to help protect your personal information. We also encourage you to activate the Identity Monitoring services being offered to you through Kroll, which are free to you upon activation. You will need to reference the membership number in this letter when activating, so please do not discard this letter.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your Identity Monitoring services.

You have until <<b2b\_text\_6 (activation date)>> to activate your Identity Monitoring services.

Kroll Membership Number: <<Membership Number s\_n>>

For more information about Kroll and your Identity Monitoring services, you can visit [info.krollmonitoring.com](http://info.krollmonitoring.com).

Additional information describing your services is included with this letter.

**For more information.** If you have any questions about this incident or the complimentary services being offered to you, please contact our dedicated call center at (866) 373-8998, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays. Please have your Kroll membership number ready.

We take the privacy and security of all information within our possession very seriously. Please accept our sincere apologies and know that 1st Source deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink that reads "Andrea G. Short". The signature is written in a cursive, flowing style.

Andrea G. Short  
President and CEO

1st Source Bank  
100 N Michigan St  
South Bend, IN 46601

## STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

**Review Your Account Statements and Notify Law Enforcement of Suspicious Activity:** As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and 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 also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

**Copy of Credit Report:** You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, 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 also can contact one of the following three national credit reporting agencies:

### **Equifax**

P.O. Box 105851  
Atlanta, GA 30348  
1-800-525-6285  
[www.equifax.com](http://www.equifax.com)

### **Experian**

P.O. Box 9532  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

### **TransUnion**

P.O. Box 1000  
Chester, PA 19016  
1-800-916-8800  
[www.transunion.com](http://www.transunion.com)

**Fraud Alert:** 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 one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

**Security Freeze:** You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

**Additional Free Resources:** You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

### **Federal Trade Commission**

600 Pennsylvania Ave, NW  
Washington, DC 20580  
consumer.ftc.gov, and  
[www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)  
1-877-438-4338

### **Maryland Attorney General**

200 St. Paul Place  
Baltimore, MD 21202  
oag.state.md.us  
1-888-743-0023

### **New York Attorney General**

Bureau of Internet and Technology  
Resources  
28 Liberty Street  
New York, NY 10005  
1-212-416-8433

### **North Carolina Attorney General**

9001 Mail Service Center  
Raleigh, NC 27699  
ncdoj.gov  
1-877-566-7226

### **Rhode Island Attorney General**

150 South Main Street  
Providence, RI 02903  
<http://www.riag.ri.gov>  
1-401-274-4400

### **Washington D.C. Attorney General**

441 4th Street, NW  
Washington, DC 20001  
oag.dc.gov  
1-202-727-3400

**You also have certain rights under the Fair Credit Reporting Act (FCRA):** These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.



## TAKE ADVANTAGE OF YOUR CREDIT AND 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.

### **Web Watcher**

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

### **\$1 Million Identity Fraud Loss Reimbursement**

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

### **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to 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.