

November 29, 2023

**VIA ONLINE SUBMISSION**

Attorney General Aaron Frey  
SECURITY BREACH NOTIFICATION  
6 State House Station  
Augusta, ME 04333

RE: Data Incident Notification

Dear Attorney General Frey:

Our firm represents Park Bank (the “Bank”), a Wisconsin financial institution. The Bank hereby formally submits notification of a recent data incident pursuant to Maine Rev. Stat. Tit. 10, Section 210-B-1346 et seq. The Bank reserves the right to supplement this notice with any significant details learned subsequent to this submission. By providing this notice, the Bank does not waive any rights or defenses regarding the applicability of Maine law, including the applicability of Maine Rev. Stat. Tit. 10, Section 210-B-1346 et seq., the applicability of any other laws of this or any other state, or the existence of personal jurisdiction over the Bank.

On October 11, 2023, the Bank learned of an incident involving one of its third-party vendors. The incident was related to vulnerabilities discovered in the MOVEit Transfer tool by Progress Software, the commonly used secure Managed File Transfer (MFT) software supporting file transfer activities by thousands of organizations around the world. The MOVEit Transfer software was used to support the Bank’s services. The vendor’s analysis to date has identified unauthorized activity in the relevant MOVEit Transfer environment between May 27 and May 31, 2023. The investigation revealed evidence that an unauthorized third party potentially accessed the personal information of some of the Bank’s clients, including the personal information of a Maine resident. Such personal information included the resident’s name, account number, and address.

In light of the foregoing and out of an abundance of caution, the Bank has decided to notify your office (via this letter) while the Bank’s third-party vendor sent notification to the one (1) Maine resident potentially affected by this incident via U.S. Mail on or about November 29, 2023. A sample of the notification letter is attached hereto as Exhibit A.

In addition to providing notice to you through this letter, the Bank took immediate steps once notified to launch a comprehensive investigation, identify individuals affected, and notify regulatory bodies as required. The Bank received assurances from its vendor that they have remediated all technical vulnerabilities and patched systems in accordance with the MOVEit

Attorney General Aaron Frey  
November 29, 2023  
Page 2

software provider's guidelines. Furthermore, the Bank arranged for Kroll to provide complimentary identity monitoring services to affected individuals.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

GODFREY & KAHN, S.C.

A handwritten signature in black ink, appearing to read 'Sarah A. Sargent', with a large, stylized flourish at the end.

Sarah A. Sargent

SAS:cg  
Enclosure

30233484.3



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

#### **What Happened?**

At Park Bank, we take the privacy and security of our clients' personal information seriously. For that reason, we are contacting you regarding a recent data security incident involving one of our third-party vendors. On October 11, 2023, we learned of an incident related to vulnerabilities discovered in MOVEit Transfer by Progress Software, the commonly used secure Managed File Transfer (MFT) software supporting file transfer activities by thousands of organizations around the world. The MOVEit Transfer software was used to support our institution's services.<sup>1</sup>

Our vendor's analysis to date has identified unauthorized activity in the relevant MOVEit Transfer environment between May 27 to 31, 2023, which was before Progress Software publicly disclosed the existence of this vulnerability. During that time, unauthorized actors obtained files transferred via MOVEit Transfer.

#### **What Information Was Involved?**

We conducted a careful review of the contents of the files and, determined that one or more of the files may have contained information including <<b2b\_text\_3(name, data elements)>>.

#### **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, we took immediate steps to launch a comprehensive investigation, identify individuals affected and notified regulatory bodies as required. To help prevent something like this happening again we have, through our vendor, remediated all technical vulnerabilities and patched systems in accordance with the MOVEit software provider's guidelines. Our service provider also mobilized a technical response team to examine the relevant MOVEit Transfer systems and ensure that there were no further vulnerabilities.

#### **What You Can Do.**

We have arranged for you to receive a complimentary 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 an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

For more information on identity theft 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 follow this letter.

<sup>1</sup>This notice was not delayed due to law enforcement.

As a best practice, 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 statements and notify us or any other of your financial institutions if you suspect any unauthorized activity.

**For More Information.**

Please be assured that we 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 us at 1-608-663-1102, Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

A handwritten signature in cursive script, appearing to read "Suzanne Johnson".

Joshua Marron, President and Chief Banking Officer  
Suzanne Johnson, FVP Branch Banking

## 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, visit [info.krollmonitoring.com](http://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](http://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](http://www.equifax.com)

Experian:  
Credit Fraud Center  
P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion:  
Fraud Victim Assistance Department  
P.O. Box 2000  
Chester, PA 19022-2000  
1-800-680-7289  
[www.transunion.com](http://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](http://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 <https://www.marylandattorneygeneral.gov/>.

**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/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf> or [www.ftc.gov](http://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.