



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Rebecca J. Jones
Office: (267) 930-4839
Fax: (267) 930-4771
Email: rjones@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

September 28, 2023

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Capital Bank N.A. (“Capital Bank”) located at 2275 Research Blvd, Suite 600, Rockville, MD 20850, and are writing to notify your office of an incident that may affect the security of certain personal information relating to one hundred and thirty-eight (138) Maryland residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Capital Bank does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about May 31, 2023, Progress Software disclosed a zero-day vulnerability impacting Internet-exposed transfer instances utilizing the MOVEit Transfer tool for all organizations that use this software, including Capital Bank’s vendor, Fiserv. On or about August 3, 2023, Fiserv notified Capital Bank that there was unauthorized access to Fiserv’s MOVEit Transfer server between May 27 to May 31, 2023, and during that time unauthorized individuals obtained files containing information relating to Capital Bank’s customers. Capital Bank immediately requested more information from Fiserv regarding this incident. On August 10, 2023, Fiserv provided an initial communication with the identities of Capital Bank’s impacted customers, and Capital Bank

immediately conducted a review of that initial information. On September 6, 2023, Fiserv advised that additional Capital Bank data was determined to be in the scope of the incident and that they are investigating to confirm the nature of that information. Should it be determined that additional legally protected information was impacted as a result of this incident, Capital Bank will promptly take steps to notify the impacted individuals and will update this notice as needed.

The information that could have been subject to unauthorized access includes name and bank account number.

Notice to Maryland Residents

On or about September 28, 2023, Capital Bank began providing written notice of this incident to one hundred and thirty-eight (138) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Capital Bank moved quickly to investigate and respond to the incident and identify potentially affected individuals. Fiserv is providing access to credit monitoring services for two (2) years, through Kroll, a global leader in risk mitigation and response whose team has extensive experience helping people who have sustained an unintentional exposure of confidential data, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Capital Bank is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Capital Bank is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Capital Bank is providing written notice of this incident to relevant state and federal regulators, as necessary. Capital Bank has notified the Office of the Comptroller of Currency.

Office of the Attorney General
September 28, 2023
Page 3

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4839.

Very truly yours,

A handwritten signature in black ink, appearing to read "Rebecca Jones", is written over a light gray rectangular background.

Rebecca J. Jones of
MULLEN COUGHLIN LLC

RJJ:ncl
Enclosure

EXHIBIT A



2275 Research Boulevard, Suite 600
Rockville, MD 20850
855-518-2742
www.capitalbankmd.com

<<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>>,

Capital Bank N.A. (“Capital Bank” or “we” or “us” or “our”) is contacting you to notify you of an incident that occurred with one of our vendor’s software providers, which may affect some of your personal information. We have no evidence that your information has been used to commit identity theft or fraud. We are providing you with this notice to make you aware of this incident, the steps we have taken in response, and additional steps you may want to take to help protect your personal information, should you feel it is appropriate to do so.

What Happened? Fiserv (also referred to below as “the vendor”), a third-party service that provides core banking payment and financial services technology to the banking industry, including us, utilizes a third-party tool from the software provider Progress Software. One of these tools that the vendor utilizes from Progress Software is MOVEit Transfer, which is a secure software supporting file transfer activities used by thousands of companies around the world. On or about May 31, 2023, Progress Software disclosed a zero-day vulnerability impacting Internet-exposed transfer instances utilizing the MOVEit Transfer tool for all companies that use this software, including the vendor. A zero-day vulnerability means that a flaw existed in the MOVEit software, and unauthorized individuals discovered it before Progress Software knew about the flaw and had an opportunity to fix it first. On or about August 3, 2023, Fiserv notified us that there was unauthorized access to its MOVEit Transfer environment between May 27 to May 31, 2023, and during that time unauthorized individuals obtained files containing information relating to our customers. We immediately requested more information from the vendor regarding this incident. On August 10, 2023, Fiserv provided an initial communication with the identities of our impacted customers, and we immediately conducted a review of that initial information, and then again on September 6, 2023, they advised that additional Capital Bank data was determined to be in the scope of the incident and that they are investigating to confirm the nature of that information. Should it be determined that additional legally protected information pertaining to you was impacted as a result of this incident, we will promptly take steps to notify you. We understand that in response to this incident, the vendor has taken the steps prescribed by Progress Software to address the vulnerability that allowed this incident to occur and has taken further steps to increase the security of its systems going forward.

What Information Was Involved? As of this writing, Fiserv has communicated to us that your name and your Capital Bank account number was impacted during this incident. **To date, we are not aware of any unauthorized access to any client funds. If you detect any unusual or suspicious activity within your account, please reach out to Capital Bank customer service at 1-844-360-3688 immediately.**

What We Are Doing. We take this incident and the security of personal information entrusted to us very seriously. Upon the vendor’s notification of this incident, we took immediate steps to investigate this incident and we continue to do so. In the event the vendor provides additional information, we will immediately review all new information provided to us. We are also notifying state and federal regulators as required. As an added precaution, the vendor is offering you complimentary access to two years of credit monitoring services through Kroll. 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. You will need to enroll yourself in these services if you wish to do so, as we are not able to activate them on your behalf. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Information* for additional detail on these services.

What You Can Do. We encourage you to remain vigilant against instances of identity theft and fraud over the next twelve to twenty-four months by reviewing your account statements and immediately report any suspicious activity or incidents of suspected identity theft or fraud to Capital Bank. We also encourage you to review the enclosed *Steps You Can Take to Protect Personal Information* and enroll in the credit monitoring services being offered to you. In addition, we encourage you to promptly report any suspected incidents of identity theft to local law enforcement, the Federal Trade Commission, and/or your state Attorney General.

For More Information. If you have questions that are not answered by this letter, you may call Kroll's dedicated assistance line at (866) 731-2928, available Monday through Friday, from 9:00 a.m. to 6:30 p.m., Eastern Time. Additionally, you can write to us at Capital Bank N.A. 2275 Research Blvd. Suite 600, Rockville, MD 20850.

We sincerely regret any inconvenience this incident may cause you. At Capital Bank, your security and peace of mind are of utmost importance to us, and we remain steadfast in our commitment to protect your personal information.

Sincerely,

Capital Bank, N.A. Customer Service

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

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>>



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.

Monitor Your Accounts

We advise you to remain vigilant against identity theft and fraud over the next 12 to 24 months by reviewing all account statements and monitoring free credit reports. If you discover or suspect fraudulent activity involving your account, credit or debit card, we encourage you to promptly contact the issuing bank or relevant financial institution. The number to call for assistance is usually on the back of the card.

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you may need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert P.O. Box 105069, Atlanta, GA 30348-5069	Experian Fraud Alert P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.marylandattorneygeneral.gov.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are no Rhode Island residents impacted by this incident.