ECKERT SEAMANS
ATTORNEYS AT LAW

Eckert Seamans Cherin & Mellott, LLC
U.S. Steel Tower
600 Grant Street, 44th Floor
Pittsburgh, PA 15219

TEL: 412 566 6000
FAX: 412 566 6099

January 29, 2024

VIA FIRST CLASS MAIL

Attorney General John Formella
Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, New Hampshire 03301

Re: Notice of Data Security Incident

Dear Attorney General Formella:

This notice is provided by Citizens Savings Bank ("CSB"), following an incident that impacted CSB's vendor, Fiserv. This incident involved the name, financial account number and routing number of one (1) New Hampshire resident. Fiserv provided written notice to the impacted individual via U.S. Mail on January 24, 2024. The notice letter includes general advice on how to protect one's identity and obtain free credit reports and security freezes, as well as instructions for enrolling in a t complimentary membership with Kroll for credit monitoring and identity theft services. A copy of the notice letter is enclosed and additional details on the incident are below.

On November 13, 2023, Fiserv alerted CSB that certain CSB data was impacted by a cyber incident involving the MOVEit Transfer. This incident involved unauthorized access to personal information through a vulnerability in the MOVEit Transfer software. The unauthorized access occurred between May 27 and May 31, 2023. This incident did not impact CSB's computer network. On November 16, 2023, Fiserv first provided CSB with information regarding the impacted individuals and the data related to those individuals. Since that date CSB has been working to obtain details from Fiserv about this incident, to ascertain when the notice would be provided to individuals, and to ensure the accuracy of the content of those notice letters so that CSB could provide accurate and complete notices to regulators and respond to customer inquiries. However, as CSB was working through the notification process with Fiserv, it recently learned that on January 24, 2023, Fiserv mailed written notice to CSB customers and others who were impacted by this incident without prior notification to CSB. Upon discovering this, CSB moved to provide notice to all required state regulators.

Please do not hesitate to contact me if you have any questions or concerns.

Sincerely,

/s/ Matthew H. Meade, Esq.

MHM/
Enclosure

January 24, 2024

10 2 2879 ********** AUTO**5-DIGIT 18411

[redacted]

NOTICE OF DATA BREACH

Dear [redacted]

What Happened?

We are contacting you regarding an incident involving MOVEit Transfer through which some of your personal information was disclosed to a third party. On October 16, 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.

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 which included certain personal information.

What Information Was Involved?

From a careful review of the contents of the files, we have determined that one or more of the files may have contained information including .

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, our service provider has 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 . 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.

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 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 (866) 731-2928, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

CITIZENS SAVINGS BANK

ATTACHMENT A

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
You have until *to activate your identity monitoring services.*
Membership Number: [redacted]

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

KROLL

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:	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 1-877-382-4357; 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.