MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

19109 West Catawba Avenue, Suite 200
Cornelius, NC 28031

January 5, 2024

VIA E-MAIL

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301
E-mail: DOJ-CPB@doj.nh.gov

Re: Notice of Data Event

To Whom It May Concern:

We represent Woodsville Guaranty Savings Bank ("WGSB"), located at P.O. Box 266, Woodsville, NH 03785, and are writing to notify your office of an incident that may affect the security of certain personal information relating to approximately six hundred eighty-one (681) New Hampshire 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, WGSB does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On August 8, 2023, WGSB's third-party vendor, Fiserv, informed WGSB of an incident related to vulnerabilities in Fiserv's MOVEit Transfer software that affected certain WGSB data stored by Fiserv. Upon learning of this incident, WGSB promptly commenced its own investigation, with the assistance of third-party forensic specialists, which confirmed that WGSB's own systems were unaffected. One September 25, 2023, Fiserv completed its internal review of the impacted data and provided WGSB with a list of impacted individuals whose data was potentially subject to unauthorized access and/or exfiltration. WGSB then conducted an internal process of reviewing and validating this data to verify address information and provide notification to impacted individuals. This process was completed on October 16, 2023.

The information that could have been subject to unauthorized access includes

Notice to New Hampshire Residents

On or about January 5, 2024, WGSB provided written notice of this incident to six hundred eighty-one (681) New Hampshire 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 receipt of notice of this event from Fiserv, WGSB moved quickly to investigate and respond to the incident, assess WGSB's own systems to confirm that they were not affected, and review and verify the data from Fiserv regarding impacted individuals whose data was stored by Fiserv. Further, WGSB notified federal law enforcement and its state and federal regulators regarding the event. WGSB ended its relationship with Fiserv shortly after its investigation into this event concluded. WGSB is providing access to credit monitoring services for , through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, WGSB 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. WGSB 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.

WGSB is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at .

Very truly yours,

Matthew V. Toldero of
MULLEN COUGHLIN LLC

MVT/cml
Enclosure

EXHIBIT A

<<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>>,

Woodsville Guaranty Savings Bank ("WGSB") is writing to inform you of an event that may affect the security of some of your personal information. Please note that this event occurred *solely* at WGSB's third-party vendor, which is a Fortune 500 company. The event had no impact on WGSB's systems and was not the result of any activities at WGSB. Nonetheless, we are writing to provide details about the event, our response, and resources available to you to help protect your personal information from possible misuse, should you feel it is appropriate to do so.

What Happened?

On August 8, 2023, our vendor notified us of an incident related to vulnerabilities they discovered in their MOVEit Transfer by Progress Software, a 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 third-party vendor's services.

The investigation conducted by our vendor identified suspicious activity in our vendor's use of the MOVEit Transfer by Progress Software—between May 27 to 31, 2023. During that time, unauthorized actors obtained certain files held by our vendor. On September 25, 2023, our vendor completed their internal review of the impacted data and provided us with a list of the impacted individuals as a result of the event. Following receipt of this event, we worked as quickly as possible to verify the address information of these individuals and provide notification to you.

What Information Was Involved?

We were notified that one or more of the files may have contained information of yours including <<b2b_text_3(name, data elements)>>.

What We Are Doing.

We want 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. We engaged outside cybersecurity specialists to ensure that WGSB's own systems were unaffected. We understand that our third-party vendor that experienced this incident has remediated all technical vulnerabilities and patched systems in accordance with the MOVEit software provider's guidelines. Our third-party vendor also mobilized a technical response team to examine the relevant MOVEit Transfer systems and ensure that there were no further vulnerabilities. Additionally, WGSB has ended its relationship with the third-party vendor involved in this incident.

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.

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 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays.

Sincerely,

James E. Graham
President & Chief Executive Officer
Woodsville Guaranty Savings Bank

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.

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:
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 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 276999001; (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.

Rhode Island Residents: The Attorney General may be reached at: 150 South Main Street, Providence, RI 02903, (401) 274-4400 or http://www.riag.ri.gov/. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately ## Rhode Island residents that may be impacted by this event.