Goodwin Procter LLP
1900 N Street, NW
Washington, DC 20036

goodwinlaw.com
+1 202 346 4000

October 23, 2023

New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
VIA EMAIL: DOJ-CPB@doj.nh.gov

Re: Notice Pursuant to *N.H. Rev. Stat. Ann. §§ 359-C:19, C:20, C:21*

Dear Attorney General Formella,

Pursuant to *New Hampshire Revised Statutes Annotated sections 359-C:19, C:20* and *C:21*, we write on behalf of Bank of Canton, a regional bank that offers financial services primarily to Massachusetts residents, to notify you of a data security matter arising from the MOVEit vulnerability, which in this case impacted one of Bank of Canton's service providers, a publicly traded company which serves thousands of businesses in the financial industry. We believe this matter has impacted approximately forty-one **(41)** New Hampshire residents. Bank of Canton is located at 490 Turnpike St. Canton, MA 02021.

In late May 2023, Progress Software discovered a previously unknown critical vulnerability affecting its MOVEit Managed File Transfer application. MOVEit is a widely used software that allows for the transfer of files and data among businesses. As you are likely aware, many companies have been impacted by the MOVEit vulnerability, including Bank of Canton's provider. On or around August 3, 2023, Bank of Canton's provider informed the bank that certain data that the provider stored on behalf of Bank of Canton was potentially obtained as a result of the MOVEit vulnerability. In response, Bank of Canton promptly launched an investigation and requested additional information from the provider to assess the impact to its customers. On or around August 10, 2023, the provider informed Bank of Canton that the personal information of certain Bank of Canton customers was impacted in this security event but advised that its investigation was ongoing and that it would provide additional relevant details as they arose. Bank of Canton determined on September 22, 2023 that it had reasonably sufficient information to accurately identify affected individuals and, on or around October 10, 2023, that it had reasonably sufficient information to accurately notify those individuals.

The types of personal information that may have been impacted during this incident includes: . This information was stored in an unstructured, technical format which could only be identified if successfully parsed and digested. While public reports indicate that the threat actor group credited with the MOVEit malicious activity leaks stolen data on the dark web, at this time, we have no evidence that the personal information of the impacted residents has been misused as a result of this incident.

Notification of this matter was mailed to the impacted residents on or around October 20, 2023. A copy of this notification is attached.

Bank of Canton takes the protection of customer information seriously. Bank of Canton continues to monitor the accounts of impacted customers for indications of unusual activity. The provider has advised Bank of Canton that it has addressed all technical vulnerabilities and remediated this event in

accordance with guidance from Progress Software. Bank of Canton's provider is also offering two years of identity protection services, at no cost, to affected customers through Kroll.

Should you have any questions about this matter, please do not hesitate to contact me directly, by phone or email. Thank you for your attention to this matter.

Sincerely,

Kaylee Cox Bankston

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

RE: Notice of Data Security Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to notify you about a recent cyber incident that impacted numerous companies around the world, including one of our service providers, a major, publicly traded company which serves thousands of businesses in the financial industry. Although at this time there is no indication that your personal information has been misused in relation to this event, this letter is intended to provide you with the details of what happened, the measures we have taken in response, and information on steps you may consider taking to help protect your information.

What Happened?

Progress Software recently discovered a previously unknown critical vulnerability affecting its MOVEit Managed File Transfer application. MOVEit is a widely used software that allows for the transfer of files and data among businesses. As you might have seen in the news, many companies have been impacted by the MOVEit vulnerability, including one of our third-party service providers (the "Provider"). On or around August 3, 2023, the Provider notified us that the Provider suffered a cybersecurity incident resulting from MOVEit that occurred on or around May 27, 2023. We immediately initiated communications with the Provider to understand the scope and impact of this matter. The Provider has advised us that it is in the process of conducting a comprehensive and detailed review to determine the nature of data impacted and identity of affected customers. We have been in close communication with the Provider throughout this process and, on or around September 22, 2023, we determined that we had reasonably sufficient information to accurately identify and notify affected Bank of Canton customers. Specifically, the Provider has informed us that certain information, which the Provider stored on behalf of Bank of Canton, was potentially obtained as a result of the MOVEit vulnerability. The Provider has further informed us that information of certain Bank of Canton customers was contained within the data. Based on the Provider's review, we have determined that your information may have been included.

What Information Was Involved?

The potentially impacted data include information related to your Bank of Canton deposit account(s). This information was stored in an unstructured, technical format but, if successfully parsed and digested, identifies your Bank of Canton . At this time, we do not have any evidence that any individuals have experienced fraud or misuse as a result of this matter.

What We Are Doing

We take the protection of your information very seriously. As soon as we learned of this incident from the Provider, we promptly took steps to obtain the necessary information from them so that we could notify affected individuals. We continue to work with the Provider to understand the scope of the event and steps that the Provider is taking to address it. The Provider has also informed us that it has patched the technical vulnerabilities related to the MOVEit software and remediated this event in accordance with the MOVEit software provider's guidelines.

We will continue our customary monitoring for unusual activity through the various automated fraud detection and analytical tools already in place. As an added precautionary measure, the Provider has agreed to offer you complimentary access to of identity monitoring provided through Kroll. The services are being offered to

you at no charge and include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Additional details regarding the services and how to enroll are provided below.

What You Can Do

There are steps you can take to protect yourself, including enrolling in the free identity protection services we are offering. For instructions on activating the complimentary two-year membership and additional resources and steps you can take to protect your information, please review Attachments A, B and C to this letter. Please note that you have 90 days to take advantage of the free enrollment in the credit monitoring service.

Additionally, we offer you security alerts through online or mobile banking. If you are not already enrolled, you should activate this service, which can be used to alert you to attempted changes to your accounts. It is also a good practice to regularly monitor your account(s) for any suspicious activity.

Questions or Concerns

Your relationship and the security of your account(s) are of the utmost importance to us. If you have any questions, please contact us at Monday through Friday, from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major holidays.

Thank you for banking with Bank of Canton.

Sincerely,

Peter M. Shea, SVP Operations
Bank of Canton

ATTACHMENT A

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.

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 RESOURCES

The following provides additional information and actions that you can consider taking to help protect your information. You may also contact the U.S. Federal Trade Commission ("FTC"), the credit reporting agencies, or your state's regulatory authority to obtain additional information about avoiding identity theft, including information about fraud alerts and security freezes, as further detailed below. Contact Information for the Federal Trade Commission and credit reporting agencies is set forth below:

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

Credit Reporting Agencies

Equifax	**Experian**	**TransUnion**
PO Box 740241	PO Box 4500	PO Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
1-800-525-6285	1-888-397-3742	1-800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

Order Your Free Annual Credit Report. You can order your free annual credit report online at www.annualcreditregort.com. by phone (toll free) at 877-322-8228, or by mail by submitting a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download a copy of the request form on the FTC website: www.ftc.gov. You can also visit the Consumer Financial Protection Bureau's website for more information on how you can obtain your credit report for free: www.consumerfinance.gov. Once you receive your credit reports, review them carefully for any discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting agency.

Review Your Accounts and Report Unauthorized Activity. We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the FTC. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also consider filing or obtaining a police report.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from potential identity theft, you may consider placing a fraud alert on your credit file. A fraud alert is intended to make it more difficult for someone to open a new credit account in your name. A fraud alert indicates to an entity requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the alert notifies the entity to take steps to verify your identity. You may contact one of the credit reporting agencies listed above for assistance.

Consider Placing a Security Freeze on Your Credit File. You also may consider implementing a security freeze (also called a "credit freeze"). Placing a freeze on your credit report restricts access to your credit report and will prevent lenders and others from accessing your credit report entirely. This means you (or others) will not be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. With a security freeze in place, you may be required to take special steps when you wish to apply for any type of credit. You may contact one of the credit reporting agencies listed above for assistance.

Remain Vigilant and Lookout for Phishing Schemes. We also encourage you to remain vigilant in managing and handling your personal information and be on the lookout for suspicious emails, such as phishing schemes. Phishing schemes are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which are actually sent by a fraudulent impersonator. Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the

email address (e.g., look for misspellings). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate. Also consider taking steps such as carrying only essential documents with you, being aware of how and with whom you are sharing your personal information, and shredding receipts, statements, and other sensitive information once you no longer need them.

For District of Columbia Residents: You may also obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia:

Office of the Attorney General for the District of Columbia
Office of Consumer Protection
400 6th Street NW
Washington, D.C. 20001
(202) 442-9828
https://oag.dc.gov/

For Maryland Residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
http://www.marylandattorneygeneral.gov

For residents of New York: You may also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office or New York's Office of Information Technology Services:

New York Attorney General's Office
Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755
https://ag.ny.gov/

New York Office of Information Technology Services
Empire State Plaza
P.O. Box 2062
Albany, NY 12220-0062
844-891-1786
https://its.ny.gov/

For North Carolina Residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-5-NO-SCAM
www.ncdoj.gov

For Rhode Island Residents: You have the right to obtain a police report. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Rhode Island Office of the Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
1-401-274-4400
https://riag.ri.gov/

ATTACHMENT C

For Massachusetts Residents Only

Under Massachusetts law, you have the right to obtain any police report filed in regard to this 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. You may also place a security freeze on your credit reports, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, 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. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

You must place your request for a freeze with each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com). To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail at the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/	P.O. Box 9554 Allen, TX 75013 1-888-397-3742 https://www.experian.com/freeze/center.html	P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 https://www.transunion.com/credit-freeze

In order to request a security freeze, you will need to provide some, or all, of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

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, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2; and
8. 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.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.