January 8, 2024

VIA EMAIL

Attorney General John M. Formella
Office of the Attorney General
Consumer Protection & Antitrust Bureau
1 Granite Place South
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General Formella:

My firm represents Bank of New England, a financial company with a principal place of business located at 31 Pelham Road, PO Box 29, Salem, New Hampshire. Pursuant to N.H. RSA § 359- C:20, Bank of New England notified its primary regulatory authority, the Federal Deposit Insurance Company, as well as the New Hampshire Banking Department ("Banking Department"), of a data breach. The Banking Department has asked that the bank also notify you. As such I am writing to notify you of a data breach involving the personal information of 2,483 New Hampshire residents.

On October 20, 2023, Bank of New England was informed by its service provider, Fiserv, of an incident through which certain account and personal information of individuals was disclosed to a third party. As part of its service to Bank of New England, Fiserv used MOVEit Transfer by Progress Software, a commonly used secure Managed File Transfer software supporting file transfer activities by thousands of organizations around the world. A previously unknown vulnerability in MOVEit Transfer software allowed unauthorized activity between May 27 to 31, 2023. During that time, unauthorized actors obtained data belonging to hundreds of organizations. Included in the data obtained by unauthorized actors was personal identifiable information ("PII") of Bank of New England customers, including 2,483 New Hampshire residents. At this time, Bank of New England has not received any evidence that the confidential information that was taken has been misused.

As a result of this chain of events, the unauthorized actors may have had access to PII including individuals'

At the time of the incident, Bank of New England maintained a written information security program.

Upon learning of this incident, Bank of New England 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, Fiserv has remediated all known

technical vulnerabilities and patched the MOVEit Transfer application in accordance with the MOVEit software provider's guidelines. Fiserv also mobilized a technical response team to examine the relevant MOVEit Transfer systems to ensure that there were no further vulnerabilities.

The affected individuals have been notified of the incident by a written notice. A copy of the written consumer notice letter is attached.

of credit monitoring services have been offered to the affected individuals.

If you should have any question or require any additional information regarding this incident, please feel free to contact me.

Very truly yours,

Seth Berman

SPB2:np
Enclosure
6310992.1

BANK OF NEW ENGLAND
31 Pelham Road, PO Box 29, Salem, NH 03079
Tel: 603-894-5700 Fax: 603-894-5757

<<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>> <<Last_Name>>,

At Bank of New England, we take security of your data very seriously and value the relationship that we have with you. We are reaching out to you today to inform you of a data breach at a third-party service provider, Fiserv, utilized by the Bank, which resulted in the exposure of some of your confidential information.

At this time, Bank of New England has not received any evidence that the confidential information that was taken has been misused. We believe it is crucial that we keep you informed and that you take precautionary measures that are available to you herein. Please read this letter carefully for information about the incident and learn how you can take steps to help protect yourself against the possible misuse of the information. We strongly encourage you to take advantage of the services described below and we recommend that you change any passwords associated with your accounts, as well as continue to monitor your accounts for any unusual activity.

Please be assured that we are taking all of the necessary steps to address the incident and to help protect the security of your data. We deeply regret any inconvenience this may have caused.

If you have any questions or concerns about this notice and/or the incident, please feel free to contact us directly.

What Happened?

On October 20, 2023, Bank of New England was informed by our service provider of an incident through which certain account and personal information of yours was disclosed to a third party. As part of its service to Bank of New England, the service provider used 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. A previously unknown vulnerability in MOVEit Transfer software allowed unauthorized activity between May 27 to 31, 2023. During that time, unauthorized actors obtained data belonging to hundreds of organizations. Included in the data obtained by unauthorized actors was confidential information about Bank of New England customers including your personally identifiable information.

What Information Was Involved?

The Bank of New England information involved in this incident included your <<b2b_text_3 (name, impacted 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, the service provider has remediated all known technical vulnerabilities and patched the MOVEit Transfer application in accordance with the MOVEit software provider's guidelines. The service provider also mobilized a technical response team to examine the relevant MOVEit Transfer systems to 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.

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 Kroll at [TFN], Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

Bank of New England

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:	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.

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.

BANK OF NEW ENGLAND
31 Pelham Road, PO Box 29, Salem, NH 03079
Tel: 603-894-5700 Fax: 603-894-5757

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

To the Parent or Guardian of
<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

NOTICE OF DATA BREACH

Dear Parent or Guardian of <<First_Name>> <<Last_Name>>,

At Bank of New England, we take security of your child's data very seriously and value the relationship that we have with you. We are reaching out to you today to inform you of a data breach at a third-party service provider, Fiserv, utilized by the Bank which resulted in the exposure of some of your child's confidential information.

At this time Bank of New England has not received any evidence that the confidential information that was taken has been misused. We believe it is crucial that we keep you informed and that you take precautionary measures that are available to you herein. Please read this letter carefully for information about the incident and learn how you can take steps to help protect your child against the possible misuse of the information. We strongly encourage you to take advantage of the services within and we recommend that you change any passwords associated with your child's accounts, as well as continue to monitor your child's accounts for any unusual activity.

Please be assured that we are taking all of the necessary steps to address the incident and to help protect the security of your data. We deeply regret any inconvenience this may have caused.

If you have any questions or concerns about this notice and/or the incident, please feel free to contact us directly.

What Happened?

On October 20, 2023, Bank of New England was informed by the service provider of an incident through which certain account and personal information of your child's was disclosed to a third party. As part of its service to Bank of New England, the service provider used 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. A previously unknown vulnerability in MOVEit Transfer software allowed unauthorized activity between May 27 to 31, 2023. During that time, unauthorized actors obtained data belonging to hundreds of organizations. Included in the data obtained by unauthorized actors was confidential information about Bank of New England customers including your child's personally identifiable information.

What Information Was Involved?

The Bank of New England information involved in this incident included your <<b2b_text_3 (child's name, impacted 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, the service provider has remediated all known technical vulnerabilities and patched the MOVEit Transfer application in accordance with the MOVEit software provider's guidelines. The service provider also mobilized a technical response team to examine the relevant MOVEit Transfer systems to ensure that there were no further vulnerabilities.

What You Can Do.

We have arranged for your child to receive a complimentary free minor 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 child's identity monitoring services include Minor Identity Monitoring, Fraud Consultation and Identity Theft Restoration.

For more information on identity theft prevention, including instructions on how to activate your child's identity monitoring, as well as some additional steps you can take for your child's 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 child's credit history to guard against any unauthorized transactions or activity. We also recommend that you closely monitor your child's account statements and notify us or any other of your child's 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 Kroll at [TFN], Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

Bank of New England

ATTACHMENT A

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide Minor Identity Monitoring, Fraud Consultation, and Identity Theft Restoration at no cost to you 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.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your Minor Identity Monitoring services.

You have until <<b2b_text_6 (activation date)>> to activate your Minor Identity Monitoring services.

Membership Number: **<<Membership Number s_n>>**

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Minor Identity Monitoring

Minor Identity Monitoring detects when names, addresses, and credit information is associated with your child's Social Security number. An alert will be sent to you when activity is detected. The presence of a credit file may be an indicator of identity theft or fraud for children who, as minors, should not have a credit history.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to 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.

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 and to review your child's account statements. 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 security freeze on your child's credit report. If you believe your child is 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 IMPLEMENTING A CREDIT FREEZE

To place a credit freeze on your child's 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

Credit Freeze: You may place a free credit freeze for children under the age of 16. By placing a security freeze, someone who fraudulently acquires your child's personal identifying information will not be able to use that information to open new accounts or borrow money in their name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, your child will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your child's credit files.

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.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

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.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

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.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

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.

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.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

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.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

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.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.