**Seth Berman**
Direct Line: (617) 439-2338
Fax: (617) 310-9338
E-mail: sberman@nutter.com

November 7, 2022
0124451-1

**Via Email**

Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov
attorneygeneral@doj.nh.gov

Re: Notice of Data Security Incident

Office of the Attorney General:

My firm represents Eagle Bank (the "Bank"), a bank with a principal place of business located at 350 Broadway, Everett, MA 02149. Pursuant to N.H. Rev. Stat. Ann. §§ 359-C:19, C:20, C:21, I am writing to notify you of a data breach involving the personal information of five (5) New Hampshire residents.

On September 20, 2022, the Bank learned that several customers and others related to Eagle Bank had received an email purportedly sent by Eagle Bank, but in fact coming from a different domain. This email asked the recipients to download a document, purportedly from Eagle Bank. As soon as the Bank learned of the attack, the Bank's IT security team attempted (in a controlled environment) to download the suspect document to analyze it. However, the document that the link pointed to had been deactivated and could not be downloaded. Eagle Bank has no reason to believe that any customer downloaded the suspicious document (and it is not even clear if that would have been possible).

Although the email did not come from within the Bank, the fact that the recipients included actual Eagle Bank customers and other contacts prompted the Bank to investigate whether the email addresses might have ultimately come from an Eagle Bank email address. The Bank hired an outside forensics expert to assist with this investigation, and ultimately determined that a single Bank employee's email account had been accessed by unauthorized parties once, on July 30, 2022. The investigation did not find any evidence of any additional access to this account or to any other Eagle Bank email account. Indeed, by the time the Bank became aware of the incident, the impacted account's password had already been changed, pursuant to the Bank's requirement for periodic and forced rotation of account passwords. The forensic investigation was not able to determine exactly what the unauthorized individuals had done in the account, or what information they obtained from the account.

After concluding that the email account had been subject to unauthorized access, the Bank engaged additional outside experts to review the contents of the account and determine if any personal information for customers or other individuals had been present in the account. The investigation revealed that the email account included files that contained first and last names, social security numbers, drivers' license numbers, financial account numbers, and dates of birth. Though the hackers had access to the email account containing this information, the Bank is not aware of any evidence they have misused or disseminated the information.

A copy of the form of consumer notice letter is attached as Exhibit A. The notification will be sent to the New Hampshire residents on **November 8, 2022**.

The name and contact information of the person reporting the breach is:

Marc J. Whittaker
President/C.E.O.
Eagle Bank
350 Broadway
Everett, MA 02149
617.394.3616

The Bank is monitoring the accounts of all affected Eagle Bank customers for unusual activity and has offered two years of credit monitoring to any of the affected individuals. The Bank has also notified law enforcement of the incident.

As part of the Bank's ongoing efforts to help prevent a similar incident from happening in the future, the Bank has taken steps to improve its security policies and procedures, and to retrain its personnel.

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

Very truly yours,

Seth Berman

SPB2:nmc2
Enclosure
5767714.1

# EXHIBIT A

EAGLE BANK

<<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>>,

We are writing to tell you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the incident.

**What happened?**

On September 20, 2022, Eagle Bank discovered that an email account of one of its employees had been compromised by a hacker. An investigation later revealed that the hacker had accessed the account for a brief period of time on July 30, 2022. The hacker may have gained access to information in the email account, including personal information about you.

Eagle Bank has reported the incident to law enforcement and has taken steps to ensure the security of Eagle Bank accounts. We are notifying you of this incident so that you can take steps, as detailed below, to further help protect yourself.

**What information was involved?**

By hacking into an email account, the hacker may have gained access to your Social Security number and may also have gained access to other information about you, such as your date of birth, driver's license number, and/or financial account number(s).

**What we are doing.**

Eagle Bank has undertaken increased vigilance on all accounts that were potentially impacted to ensure that there are no improper withdrawals and has implemented additional security measures.

To help relieve concerns following this incident, we have secured the services of Kroll to provide identity monitoring 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. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

*You have until **<<b2b_text_6 (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.

Additional information describing your services is included with this letter.

**What you can do.**

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

**For more information.**

If you have questions, please call <<TFN>>, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding U.S. holidays. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Marc J. Whittaker
President/C.E.O.

**ADDITIONAL RESOURCES**

**Remain Vigilant and Report Suspicious Activity.** You should remain vigilant for suspicious activity, especially activity that may indicate fraud or identity theft, for at least the next 12 to 24 months. Please review your account statements for any suspicious and/or unauthorized activity. In addition, please contact us promptly to report incidents of suspected fraud or identify theft involving your account with us by calling 1-617-394-3691, Monday through Friday from 8:00 a.m. to 5:30 p.m. Eastern Time. Other steps you can take to protect your credit information are described below. The Federal Trade Commission also provides guidance to consumers about protecting against identity theft through its website: https://consumer.ftc.gov/features/identity-theft. You may also report identity theft to the Federal Trade Commission by calling 1-877-438-4338 or 1-866-653-4261 (TTY), or through the following website: http://www.identitytheft.gov.

**Contact information for the three nationwide credit reporting agencies:**

**Equifax**, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

**Experian**, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

**TransUnion**, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

**Free Credit Report.** It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

**For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

**Fraud Alerts.** There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

**Security Freeze.** You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

**Federal Trade Commission and State Attorneys General Offices.** If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

**For Maryland residents:** You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

**For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

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

**For Connecticut residents:** You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

**For Massachusetts residents:** You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

**Reporting of identity theft and obtaining a police report.**

**For Iowa residents:** You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

**For Massachusetts residents:** You have the right to obtain a police report if you are a victim of identity theft.

**For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

KROLL

**TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES**

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

**Triple Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—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 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.