BakerHostetler

Baker&Hostetler LLP

2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

David Sherman
direct dial: 215-564-8380
dsherman@bakerlaw.com

May 27, 2020

**VIA OVERNIGHT MAIL**

Gordon MacDonald
Office of the Attorney General
33 Capitol St.
Concord, NH 03301

*Re: Incident Notification*

Dear Sir or Madam:

We are writing on behalf of our client, Mabrey Bank, to notify you of a security incident.

Mabrey Bank recently concluded its investigation of an incident that involved unauthorized access to two employees' email accounts. Mabrey Bank learned on February 11, 2020 that suspicious emails requesting wire transfers were sent from one Mabrey Bank employee's email account to another employee. Upon learning of this, Mabrey Bank launched an investigation. Through its investigation, Mabrey Bank determined that the wire transfer requests were sent from the employee's email account without their knowledge. Mabrey Bank immediately reset the password to the employee's email account and a leading cybersecurity firm was engaged to assist with its investigation. Fortunately, Mabrey Bank maintains policies and procedures that help mitigate risks associated with fraudulent wire transfers, so the wire transfer requests were denied and no funds were lost.

The investigation determined that two Mabrey Bank employees inadvertently disclosed their email account credentials pursuant to phishing emails that appeared to have been legitimately sent by one of Mabrey Bank's customers. An unauthorized person then may have used the credentials to the two email accounts to login and access the employees' email accounts between January 30, 2020 and February 10, 2020. Although the likely purpose of the unauthorized access to the two employees' email accounts was to obtain funds through fraudulent wire transfers, the unauthorized person may have been able to access emails and attachments in the two accounts. Therefore, out of an abundance of caution, Mabrey Bank conducted a review of the emails and attachments in the employees' email accounts to determine what information may have been accessed by the unauthorized person.

Through this review, which was completed on April 8, 2020, Mabrey Bank determined that the unauthorized person may have accessed emails and attachments in the employees' email accounts that contained names in combination with financial account information (bank account and routing numbers).

Beginning on May 27, 2020, Mabrey Bank will mail notification letters via United States Postal Service First-Class mail to two (2) New Hampshire residents in accordance with N.H. Rev. Stat. § 359-C:20. A copy of the notification letter is enclosed.[1]

To help prevent something like this from happening in the future, Mabrey Bank has reset the passwords to the employees' accounts, increased monitoring of network activity, added additional email authentication measures and is providing additional cybersecurity training to employees.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

David Sherman

Enclosure

[1] This report is not, and does not constitute, a waiver of the Mabrey Bank's objection that New Hampshire lacks personal jurisdiction over the Mabrey Bank regarding this incident.

MabreyBank

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

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

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

Mabrey Bank is committed to protecting the confidentiality and security of the information we maintain. We are writing to inform you that we recently identified and addressed a data security incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

On April 8, 2020, Mabrey Bank concluded our investigation of an incident that involved unauthorized access to two of our employees' email accounts. Upon learning of the incident on February 11, 2020, we promptly secured the employees' email accounts and a leading cybersecurity firm was engaged to assist with the investigation. Our investigation determined that an unauthorized person may have accessed the employees' email accounts between January 30, 2020 and February 10, 2020 and may have been able to access emails and attachments in the accounts. As part of our investigation, we conducted a comprehensive review of the emails and attachments in the email accounts to identify individuals whose information may have been accessible to the unauthorized person as a result of this incident.

Through this review, we determined that the unauthorized person may have accessed your name in combination with your <<b2b_text_1 (Impacted Data)>><<b2b_text_2 (Impacted Data)>>.

We remind you to remain vigilant to the possibility of fraud by reviewing your financial account and payment card statements for any suspicious activity. You should immediately report any suspicious activity to your financial institution. Please see the pages that follow this notice for additional steps you may take.

We regret and apologize for any inconvenience or concern this may cause you. To help prevent something like this from happening in the future, Mabrey Bank has reset the passwords to the employees' accounts, increased monitoring of network activity, added additional email authentication measures and is providing additional cybersecurity training to employees.

If you have any questions, please call 1-???-???-????, Monday through Friday, between 8:00 a.m. and 5:30 p.m. Central Time, excluding major U.S. holidays, and we will be happy to help you.

Sincerely,

Scott Mabrey
Chief Executive Officer

## ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 to 24 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

**Fraud Alerts:** There are two types of general 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 one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

**Credit or Security Freezes:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

*How do I place a freeze on my credit reports?* There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

*How do I lift a freeze?* A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

## Additional information for residents of the following states:

**Connecticut:** You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

**District of Columbia:** The mailing address for Mabrey Bank's headquarters is 14821 South Memorial Bixby, OK 74008. You may contact and obtain information from your attorney general at: *Office of the Attorney General for the District of Columbia*, 441 4th Street, NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov

**Maryland:** The mailing address for Mabrey Bank's headquarters is 14821 South Memorial Bixby, OK 74008. You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

**New York:** You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

**North Carolina:** You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

**West Virginia:** You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

**A Summary of Your Rights Under the Fair Credit Reporting Act:** The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.