17471

BANK OF CANTON

We're like family.

August 18, 2020

[redacted]

Dear [redacted]:

Thank you for your continued patronage to Bank of Canton. We value and appreciate your business.

As a follow-up to our recent conversation, I am writing to inform you that a copy of the Debit / ATM Card Reissue Request that that had been completed for you on July 3, 2020 was inadvertently sent to another customer of our bank. As we discussed, the Request contained your name, social security number, address and account number.

Also, and as we discussed, I strongly encourage you to take the following steps:

1. **Close the affected account (if you have not done so already).**
2. **Continue to monitor your account.** Remain vigilant and contact us immediately at **(888) 828-1690** if you detect any unusual activity.
3. **Participate in an Identification Protection Program. Bank of Canton will cover the cost of a two-year subscription with LifeLock, the credit monitoring service you have selected. I will ensure that you are registered for this service and will reach out to you with any additional details.**

We also encourage you to notify the three major credit bureaus of this incident, and take additional steps to guard against identity theft. We have enclosed recommendations from the State and Federal governments, which include best practices to assist you. Please review them carefully.

We take our commitment to protecting customer information very seriously. Please accept our apologies for the manner in which your information has been handled. We sincerely hope that this incident has not shaken your trust in our ability to serve your financial needs. Should you require additional assistance, please contact me at (888) 828-1690, or via email at kludecker@thebankofcanton.com.

Again, thank you for your business and for placing your trust in Bank of Canton.

Sincerely,

Katherleen A. Ludecker

Katherleen A. Ludecker
Assistant Vice President / Branch Manager – Randolph Branch

Enclosures – As noted above

MASSACHUSETTS LAW ENCLOSURE

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.

Massachusetts law also allows consumers to place a security freeze on their credit reports. 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.

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554 Allen,
TX 75013

Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000

In order to request a security freeze, you will need to provide the following information:

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, provide 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.)
7. 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;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. 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.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (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 or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days 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 send a written request to each of the three credit bureaus by mail and include 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 three (3) business days after receiving your request to remove the security freeze.

THE FOLLOWING INFORMATION WHICH WAS OBTAINED FROM ON-LINE RESOURCES OF THE FEDERAL TRADE COMMISSION (FTC) MAY BE HELPFUL

If you have reason to believe your personal information has been compromised or is being misused:

1. **Contact the fraud departments of each of the three major credit bureaus.**
   - Tell them to flag your file with a fraud alert including a statement that creditors should get your permission before opening any new accounts in your name.
   - Ask them for copies of your credit reports. Credit bureaus must give you a free copy of your report if it is inaccurate because of fraud. Review your reports carefully to make sure no additional fraudulent accounts have been opened in your name or unauthorized changes have been made to your existing accounts.
   - In a few months, order new copies of your reports to verify your corrections and changes and to make sure no new, fraudulent activity has occurred.

   Credit Bureaus

   Equifax: 800-685-1111 or 800-525-6285; www.equifax.com
   Experian: 888-397-3742; www.experian.com
   TransUnion: 800-916-8800 or 800-680-7289; www.tuc.com

2. **If your credit accounts have been tampered with or if new accounts have been opened fraudulently, contact your creditors.**
   - Ask to speak with someone in the security or fraud department, and follow up in writing. Following up with a letter is one of the procedures spelled out in the Fair Credit Billing Act for resolving errors on credit billing statements, including charges that you have not made.
   - If you discover a changed billing address on an existing credit card account, close the account.
   - When you open a new account, ask that a password be used before any inquiries or changes can be made on the account. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers. Avoid the same information and numbers when you create a Personal Identification Number.

3. **If you have reason to believe that an identity thief has accessed your bank accounts, checking account, or ATM card, close the accounts immediately.**
   - When you open new accounts insist on password-only access.

4. **Check your Social Security Statement by calling 800-772-1213.**
   - If you suspect that someone is using your SSN when applying for a job, get in touch with the Social Security Administration (SSA) to verify the accuracy of your reported earnings and that your name is reported correctly.
   - If you suspect that your name or SSN is being used by an identity thief to get a driver's license, report it to your Department of Motor Vehicles.
   - If your state uses your SSN as your driver's license number, ask to substitute another number.

5. **Contact your local law enforcement agency to inquire about filing a police report.**
   - Get a copy of the report. Many creditors want the information it contains to absolve you of any fraudulent debts.
   - You should also file a complaint with the FTC at www.consumer.gove/idtheft or at 877-

438-4338. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

The FTC works to prevent fraudulent, deceptive, and unfair business practices in the marketplace while providing information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit www.ftc.gov or call toll-free 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.