

14807

March 27, 2019

Customer Address

Dear Customer:

Belmont Savings Bank (the "Bank") values your business and respects the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about an isolated data security incident that involves your personal financial information.

While we do not have any evidence that your personal financial information will be used by any other party, we are required by law to inform you of your rights in regard to protecting your confidential personal financial information.

Belmont Savings Bank values your privacy and deeply regrets that this incident occurred. We have implemented additional security measures designed to prevent a recurrence of such an incident and to protect the privacy of our valued customers.

We encourage you to remain vigilant by reviewing your account statements and credit reports closely over the next 12 to 24 months. If you detect any suspicious or unauthorized activity on your account, you should promptly notify us or the company with which the account is maintained.

Steps You Can Take To Further Protect Your Information

- **Police Report:** Under Massachusetts law, you have the right to obtain any police report filed regarding 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.
- **Security Freeze:** You have a right to request a free "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. A security freeze can be requested by sending a request either by toll-free telephone, secure electronic means or by mail to a consumer reporting agency. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze may delay, interfere with, or prevent the timely approval of any subsequent request or application you make regarding new loans, credit, mortgage, insurance, government services or payments, rental housing, employment, investment, license, cellular phone, utilities, digital signature, internet credit card transactions or other services, including an extension of credit at a point of sale.

To place a security freeze on your credit report, contact each of the nationwide consumer reporting agencies:

Equifax
Equifax.com/personal/credit-report-services

(800) 685-1111

Experian
Experian.com/help
(888) 397-3742

Transunion Security Freeze
Transunion.com/credit-help
(888) 909-8872

You will need to supply your name, address, date of birth, Social Security Number and other personal information.

After receiving your freeze request, each consumer reporting agency will provide you with a unique PIN (personal identification number) or password. Be sure to keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

When you place a security freeze on your credit report, within 5 business days of receiving your request for a security freeze, the consumer reporting agency will send you a confirmation of the security freeze. The consumer reporting agencies may not charge a fee to any consumer who elects to place, lift or remove a security freeze from their credit report.

- **Fraud Alert:** 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. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide consumer reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file.

An initial fraud alert stays in your file for at least one year. An extended alert stays in your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency, and additional information a consumer reporting agency may require you to submit. For more detailed information about the identity theft report, visit www.consumerfinance.gov/learnmore. An active duty military alert is for those in the military who want to protect their credit while deployed. This fraud alert lasts for one year and can be renewed for the length of your deployment. The consumer reporting agency will also take you off their marketing lists for pre-screened offers for two years, unless you ask them not to.

- **Free Credit Reports:** Credit reports contain information about you, including what accounts you have and your bill paying history. The law requires the major nationwide consumer reporting agencies – Equifax, Experian and TransUnion – to give you a free copy of your credit report every 12 months, if you request it. Visit www.annualcreditreport.com to order your free credit reports. It is recommended that you obtain a free copy of your credit report every 12 months from each consumer reporting agency and that you review the credit reports to ensure that the information on all your credit reports is correct and up to date. Reviewing your credit reports helps provide an early sign of potential identity theft.

You can further educate yourself regarding identity theft, security freezes, and the steps you can take to protect yourself by contacting the Massachusetts Attorney General or the Federal Trade Commission (FTC). The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (877-438-4338); and TTY: 866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them, and you can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement, the FTC, and the Massachusetts Attorney General.

We appreciate your understanding and regret any inconvenience this event may have caused. Belmont Savings Bank remains committed to safeguarding your information and will continue to take proactive steps to enhance our data security. If you should have any further questions relating to this incident, please do not hesitate to contact me at 617- 993-1464 or by email at Camille.remus@belmontsavings.com.

Sincerely,

Camille Remus
SVP/Chief Compliance Officer