Savers Bank

270 Main *St. P. O. Box 250 Southbridge, MA 01550*

Special Notice 23413

October 29, 2021
RE: Your Debit card ending in XXXX

X
X
X

Dear:

We have been notified by MasterCard International of a suspected security breach of a merchant's network, transactions that may have compromised some of Savers Bank's debit card numbers. We have not had any evidence of fraudulent activity, however, for your account protection; we are reissuing all affected cards.

- You will be receiving a **new debit card ordered on October 29, 2021**.
- Your old card will be deactivated in 15 days and should be destroyed.
  Should you want to close this card immediately, please contact our ATM Department at 1-508-765-7345
  or the Hot Card Service Center at 1-800-554-8969.
- **You will need to ACTIVATE the new card by calling the toll free number that appears on the label attached to your new card.**
- Please be aware that any automated payments or recurring transactions, which use the old CARD number, will need to be changed.
- We encourage you to sign up for ***Online Banking***, a free service to you, where you can view your accounts online, with many helpful features; get more information online at www.saversbank.com by clicking on "Online Banking" under quick links on the left side of your screen.
- As always and especially now, you should monitor your account by promptly reviewing your monthly statement, or through use of our online banking services. Report any unauthorized activity immediately. In the unlikely event fraud was to occur we have included information on how to protect yourself.
- Should you have any questions or concerns you can contact your local Savers Bank branch office or please contact us toll free at 1-800-649-3036.

We apologize for any inconvenience this may cause you.

Your privacy and confidential banking information are a priority for us at Savers Bank, and we thank you for your continued business.

Sincerely,

Savers Bank
ATM Department

IMPORTANT NOTICE ABOUT YOUR PERSONAL INFORMATION

Here are the actions we recommend you take to protect yourself:

1. You should be mindful for the next 12 to 24 months in reviewing your account statements and notify us of any suspicious activity.

2. You may contact the fraud departments of the three major credit reporting agencies to discuss your options. You should review your credit report and may obtain your report by contacting any of the credit reporting agencies listed below. You may also receive a free annual credit report at www.annualcreditreport.com. You have the right to place a free 90-day fraud alert on your credit file. A fraud alert lets creditors know to contact you before opening new accounts. It also may delay your ability to obtain credit. To place a fraud alert on your credit report contact the three credit reporting agencies below.

Experian	Equifax	TransUnion
(888) 397-3742	(877) 478-7625	(800) 680-7289
P.O. Box 9532	P.O. Box 740241	P.O. Box 6790
Allen, TX 75013	Atlanta, GA 30374-0241	Fullerton, CA 92834-6790
www.experian.com	*www.equifax.com*	*www.transunion.com*

3. You may wish to learn more about identity theft. The Federal Trade Commission has on-line guidance about the steps that consumers can take to protect themselves against identity theft. You can call 1-877-ID-THEFT (1-877-438-4338) or visit the Federal Trade Commission's website at *www.ftc.gov*, or *www.consumer.gov/idtheft* to obtain additional information. We also encourage you to report suspected identify theft to the Federal Trade Commission.

FOR MASSACHUSETTS RESIDENTS ONLY

4. Under Massachusetts law you have a right to place a security freeze on your consumer credit report. The security freeze will prohibit a consumer reporting agency from releasing any information in your consumer report without your express authorization. A security freeze may be requested by sending a request by certified mail, overnight mail or regular stamped mail to a consumer reporting agency. The security freeze is designed to prevent credit, loans or services from being approved in your name without your consent. You should be aware that using a security freeze may delay, interfere with, or prevent the timely approval of any subsequent credit request or application you make regarding new loans.

5. 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.); Social Security number and date of birth;
   2. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
   3. Proof of current address, such as a current utility bill or telephone bill;
   4. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
   5. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning the identity theft;

The credit reporting agencies have 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 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. A consumer reporting agency must allow a consumer to freeze, lift or remove a freeze from a consumer report free of charge.

6. If you discover suspicious activity on your credit report, your accounts or by any other means, you may wish to file a police report. You have a right to obtain a copy of any police report you file.

We will continue to monitor the effects of the compromise and want to ensure that you are aware of the resources available to you.

Alert Number: ADC011603-US-21-1

Date: October 29, 2021

Country of Origin: USA

Event Description

Suspected data compromise of a merchant's payment card environment

This Alert discloses the payment account numbers that were exposed to potential compromise

At-Risk Data Elements

Account Number

CVC2

Expiration Date

Cardholder Name

At-Risk Time Frame

December 1, 2019 through August 31, 2021

Previous Alert(s) Related to this Event

None

Operational Reimbursement and/or Fraud Recovery

All fraud related to this event should be reported to Mastercard in a timely manner per the Rules.

Mastercard will notify Customers who are eligible for Operational Reimbursement. Notifications will be sent to the Customer's Security Contact listed in the current edition of the Mastercard My Company Manager application for the impacted ICA.

Additional Information

If the accounts received in this alert are not valid, you may disregard this notification. Our systems can verify the BIN to ICA relationship but not determine if an account is valid or invalid.

Refer to Section 10.2 of the Mastercard Security Rules and Procedures manual for additional information on Account Data Compromise Events.

Customer Action

The file of potentially compromised accounts associated with this alert have been delivered to the Mastercard Global File Transfer endpoint for each impacted ICA and may also be accessed through MastercardConnect.com using the Mastercard Data Exchange application if configured.

Any action(s) taken by a Mastercard customer based on this information is entirely at the customer's own discretion and risk.

Each customer must assess its individual situation and exercise procedures to address any potential risk as the customer deems appropriate.