

RECEIVED

FEB 15 2024

OFFICE OF CONSUMER AFFAIRS



Main Street
BANK

February 8, 2024

Office of Consumer Affairs and Business Regulation
501 Boylston St
Suite 5100
Boston, MA 02116

To Whom It May Concern:

In compliance with Massachusetts 93H, we hereby notify you that we have been informed by the MasterCard Fraud Management department of a "SUSPECTED PHYSICAL DATA COMPROMISE OF A MERCHANT'S PAYMENT CARD ENVIRONMENT". We were informed of this breach by Mastercard via email on February 8, 2024. It is not known if the breach has been widely reported in the press.

From MasterCard, we have been notified that personal information of our customer(s) may have been included in the breach. The full magnetic strip was compromised. To date, we have been informed that the information of 1 of our debit cards have been included. Though not certain, we believe that almost all the customer(s) live in Massachusetts.

To best protect all parties involved we have sent letters to our affected customers which explain the steps we have taken to protect them as well as offer them the opportunity to reissue their debit card if they would like to do so.

We continue to monitor the situation.

Sincerely,

Carla Lembo

Carla Lembo
Digital Banking Specialist III
Direct Line: 508-460-4120
clembo@bankmainstreet.com

CC:
Office of the Attorney General
Maura Healey
One Ashburton Place
Boston MA 02108



Main Street
BANK

**IMPORTANT NOTICE ABOUT YOUR MASTERCARD DEBIT CARD
AND YOUR PERSONAL INFORMATION**

February 8, 2024

CARDHOLDER NAME
CARDHOLDER ADDRESS 1
CARDHOLDER ADDRESS 2

Dear CARDHOLDER,

This is to alert you that during **December 16, 2023 through January 18, 2024**, a "SUSPECTED PHYSICAL DATA COMPROMISE OF A MERCHANT'S PAYMENT CARD ENVIRONMENT" of personally identifiable/protected data occurred. We have reason to believe that some of our customers may have had their card data compromised (which could include card names, numbers, and card expiration dates) in the incident.

At this time, we have no reason or evidence to believe that an unauthorized individual retrieved any personal information such as social security numbers or Main Street Bank account numbers.

Main Street Bank takes its obligation to safeguard personally identifiable protected data entrusted to us very seriously and therefore deems it necessary to bring this situation to your attention. We feel we have systems in place to protect you against possible fraud, however if you would like to take extra precautions you may visit a branch for an Instant Issued card, or you may request we mail your new MSB debit card in about 10-12 business days.

If you have established automated transactions with merchants (i.e., EZ pass, health clubs, internet service providers, etc.) please remember to give them your new card number and expiration date.

Here are the actions we recommend you take to protect yourself, and what we will do to assist you:

1. You should be mindful for the next 12-24 months in reviewing your account statements and notifying us of any suspicious activity.
2. Using Main Street Bank Internet Banking will allow you to monitor your account activity, helping to ensure your account security.
3. Notify us immediately if you feel an unauthorized transaction has been charged to your account. Consumers are protected against loss due to fraud by State and Federal laws.

In addition, there are steps you may consider taking to avoid any issues about your personal information or security. 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 and 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 may delay your ability to obtain credit. To place a fraud alert on your credit report, contract the three agencies below:

Experian
(888)397-3742
PO BOX 9532
Allen TX 75013
www.experian.com

Equifax
(877)478-7625
PO Box 740241
Atlanta GA 30374
www.equifax.com

TransUnion
(800)680-7289
PO Box 6790
Fullerton CA 92834
www.transunion.com

You may wish to learn more about identity theft. The Federal Trade Commission has online guidance about the steps that consumers can take to protect themselves against identity theft. You can call 1-877-



Main Street BANK

ID-THEFT (1-877-438-4338) or visit the Federal Trade Commission website at www.ftc.gov or www.consumer.gov/idtheft to obtain additional information. We also encourage you to report suspected identity theft to the Federal Trade Commission.

Under Massachusetts law you have a right to place a security freeze on your consumer credit report free of charge. 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. This freeze is designed to prevent credit, loans, or services from being approved in your name without your consent.

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

1. Your full name, social security number and date of birth
2. If you have moved within the past 5 years, provide the addresses where you have lived over those prior 5 years.
3. Proof of current address, such as current utility bill or telephone bill
4. A copy of a government issued identification card (driver's license, ID card, military ID 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.

If you discover suspicious activity in 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.

Please be assured that Main Street Bank's systems were not in any way compromised. This circumstance is a result of a "SUSPECTED PHYSICAL DATA COMPROMISE OF A MERCHANT'S PAYMENT CARD ENVIRONMENT" **and is beyond our control**. With that said, we want you to know that **our priority is you**.

If you have any questions, please call us during normal business hours at 508-481-8300. We thank you for your business and hope that our proactive approach to this dilemma further demonstrates our commitment to you.

Sincerely,

Carla Lembo

Carla Lembo
Digital Banking Specialist III
508-460-4120
clembo@bankmainstreet.com