#14147

1/2/2019

NAME
ADDRESS
CITY ST ZIP

RE: IMPORTANT NOTICE ABOUT YOUR PERSONAL INFORMATION
ATM/Debit Card ending in xxxxxxxxxxxxXXXX

Dear Member:

We are writing to notify you of a security incident recently reported to us by Fiserv Solutions Inc., our MasterCard debit card transaction processor. Fiserv Solutions Inc., and MasterCard have informed us that your card ending in **XXXX** may have been involved; possibly permitting unauthorized access to your funds. This potential exposure occurred between the dates of **August 27, 2018 through December 3, 2018**.

St. Mary's Credit Union monitors all customer accounts using fraud-monitoring software that tracks card trends and spending behavior and will alert you or possibly deny transactions that are out of the ordinary. We are also taking additional measures to protect you. Daily limits have been lowered on your debit card to **$210** for ATM withdrawals and **$500** for POS purchases. We will mail new debit cards to all members included on the MasterCard notification. Your new card will arrive in the mail within two weeks. **We will deactivate the card you are currently using by 1/19/2019**. In the meantime, we ask that you also monitor your account activity carefully in order to detect any unauthorized transactions and inform us immediately if any are posted to your account.

Here are a few basic good practices to follow if you ever feel your identity may be compromised:
1. Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you discover suspicious activity on your credit report, on your account statements or by any other means you may wish to file a police report and obtain a copy of it.

2. You may contact the fraud departments of the three major credit-reporting agencies to discuss your options. You may obtain and review your credit report by contacting any of the credit reporting agencies listed on the enclosed *Identity Theft Protection Information Summary*.

3. 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. For more information about placing a security freeze see the enclosed *Identity Theft Protection Information Summary*.

If you have any questions, please contact the Member Service Center at 866-585-SMCU (7628). Member Service Center Representatives are available to assist you Monday through Friday from 8:00AM to 7:00PM and Saturday from 8:00AM to 1:00PM.

We apologize for any inconvenience this incident may cause and want to assure you that maintaining the security of member data is St. Mary's Credit Union's highest priority.

Sincerely,

St. Mary's Credit Union

st. mary's credit union

Identity Theft Protection Information Summary

Contact Information for Credit Reporting Agencies:

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

Services Available at Credit Reporting Agencies:
You may receive a free annual credit report at www.annualcreditreport.com, by calling 877-322-8228 or in the mail by writing to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. 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. However, it also may delay your ability to obtain credit. To place a fraud alert on your credit report, contact the three credit reporting agencies listed above.

Information about a Security Freeze Available from a Credit Reporting Agency:
What is a security freeze?
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. A security freeze may be requested by calling the credit reporting agencies, visiting each individual credit agency's website, or by submitting your request in writing to each credit reporting agency.

Information about How to Obtain a Security Freeze:
Under Massachusetts law consumers can request a security freeze by submitting the following information to the credit reporting agencies:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
- Social Security Number
- Date of Birth
- If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five year period
- Proof of current address, such as a current utility bill or telephone bill
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
- 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
- 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)

Terms and Conditions Governing Security Freeze Requests from a Credit Reporting Agency under Massachusetts law:
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.

Card Compromise FAQs

I received a letter stating that my debit card may have been compromised. What does this mean?

Data compromises occur when an individual or group of individuals gain unauthorized access to a computer system for the purpose of corrupting or stealing data. When you use your debit card at a merchant such as a store, gas station, over the Internet or on the phone, your card information is recorded into a database that is retained by the merchant for a period of time. The retained information is typically card numbers and expiration dates. The unauthorized individuals may gain access to the information that is stored and may use it to perform fraudulent activity with your debit card information.

Does this mean that I have fraud on my account?

No. It only means that your card information has potentially been compromised. While fraud resulting from a data compromise is rare, we recommend that you review your account and report any suspicious or unauthorized transaction to the credit union immediately. Online banking is a great way to monitor your account activity since it is immediate and you won't need to wait for a monthly statement.

How does St. Mary's Credit Union react to compromise notifications?

St. Mary's Credit Union takes every compromise seriously. Affected members will receive written notification if their card information has been potentially compromised. St. Mary's Credit Union evaluates the need to re-issue new debit cards to affected members. In certain circumstances, St. Mary's Credit Union will issue you a new debit card. In those cases, a close date for your compromised card will be included in the letter.

How do you know that my card was affected?

We receive notice of potentially compromised cards from MasterCard. MasterCard learns of the compromise through various sources including merchants, processors and even law enforcement.

Why don't you disclose the name of the merchant in the letter that you send me?

MasterCard does not disclose the name of the merchants or card processors that were compromised. We receive notification that an undisclosed merchant's database or processor was compromised. These breaches are investigated by law enforcement and the merchant or processor name may be disclosed at a later date.

How long will it take for me to receive a new card?

It usually takes 7 to 10 business days to receive a new debit card. Upon receipt of your card, please call (800)992-3808 to activate your card and choose your four-digit personal identification number (PIN).

What if I have preauthorized debits made to my compromised debit card number?

You should contact the merchant(s) immediately upon receipt of your replacement card and provide them with the new card number and expiration date.

There are other signers on my accounts. Does this affect their cards too?

Not necessarily. Each member has a unique card number. If their card has also been compromised, they too will receive written notification.

Can this information be used to steal my identity?

The information encoded on your debit card pertains strictly to the card, potentially including the card number and expiration date. **Confidential information such as Social Security Numbers, Driver's license numbers, addresses and dates of birth are not stored on the card.** If we are aware the merchant or processor was retaining your personal information and the information was suspected of being compromised, it will be included in the written notification you receive.

What can I do to keep this from re-occurring?

Unfortunately, we have no way of stopping criminals from "hacking" into databases of merchants or processors. While the possibility of a card being used fraudulently is low, we recognize the aggravation members face in acquiring a replacement card or having fraudulent activity removed from their account.

What should I do if I think I am a victim of identify theft?

If you detect fraud on your account, please contact St. Mary's Credit Union immediately at 1-866-585-SMCU or 508-490-8000.

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. However, it may delay your ability to obtain credit. To place a fraud alert on your credit report, contact any one of the three major credit reporting agencies.

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