17618

September 1, 2020

First and last name
Address
City, State 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 Mastercard, in which your card ending in XXXX may have been involved; possibly permitting unauthorized access to your funds. This potential exposure occurred between the dates of **February 1, 2020 through July 16, 2020**

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 have issued a new card.** Your new card will arrive in the mail within two weeks. If you do not receive your new card within two weeks from the date on this letter, please contact the Member Service Center at 866-585-SMCU (7628).
- **We will deactivate the card you are currently using by September 15, 2020.**

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 National Credit Bureaus:

Experian	Equifax	TransUnion
(888)397-3742	(800)685-1111	(888)909-8872
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 National Credit Bureaus:
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 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 one of the three national credit bureaus listed above. The credit bureau you contact will then contact the other two credit bureaus. The alert lasts one year.

Information about a Credit Freeze Available from a National Credit Bureau:
What is a credit freeze?
The credit freeze is designed to help stop anyone from opening new lines of credit in your name. You should be aware that using a credit freeze may delay, interfere with or prevent businesses from checking your credit so you may need to temporarily lift your credit freeze. You can freeze and unfreeze your credit record for free at the three national credit bureaus listed above.

Information about How to Obtain a Credit Freeze:
Under Massachusetts law consumers can request a credit freeze by submitting the following information to the national credit bureaus:

- Your full name, address, Social Security number and date of birth
- Addresses where you lived over the previous five years
- 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
- It is free to place, lift or remove a credit freeze

How long does it take for a credit freeze to go into effect?
The national credit bureaus have one (1) business day after receiving your request to place a credit freeze on your credit report if your request was made by phone or online. If the request is made by mail, the credit freeze must be placed no later than three (3) business days after receiving the request.

After five business days from receiving your credit freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place since you will need this to authorize the removal or lifting of the freeze.

If you make a request to lift or remove the credit freeze then the bureau must lift or remove the freeze:

- 1 hour after receiving the request by phone or online
- 3 business days after receiving the request by mail

Please contact the national credit bureaus for any specific requirements or instructions to place, lift or remove a credit freeze. Each credit bureau has specific requirements for placing, lifting or removing a credit 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

Manage My Fraud and Risk Programs - Account Data Compromise Notification for Nicholas Plouffe

The MasterCard Fraud Investigations department has been notified of an event in which MasterCard payment accounts have been exposed to possible compromise.

Account Compromise Summary

1.	ICA 20729	1 Accounts

Alert Number: ADC009216-US-20-1

Date: September 01, 2020

Country of Origin: United States

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

At-Risk Time Frame

- February 1, 2020 through July 16, 2020

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 Member Information Manual for the impacted ICA.

Additional Information

- If the accounts received in this alert are not valid, you may disregard this notification. Our systems are able to 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

- Go to www.MastercardConnect.com and access the Manage my Fraud and Risk Programs application to download your potentially compromised accounts and the applicable narrative for the alert.
- 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.

Disclaimer Information

The information set forth in this document is for information purposes only. Any use of this information is at user's sole risk. MasterCard disclaims any and all costs or liabilities related to this document or use thereof. MasterCard does not represent or warrant the accuracy or completeness of the information set forth in this document. This document is intended solely for use by the ICA first identified above. If you are not the intended recipient of this document, please destroy this document immediately. Any disclosure, copying, or use of the information set forth herein by anyone other than the intended recipient is prohibited and may be unlawful.