

16296

November 7, 2019

NAME
ADDRESS
CITY ST ZIP

IMPORTANT NOTICE ABOUT YOUR ST. MARY'S CREDIT UNION DEBIT CARD ending in XXXX

Dear **NAME**:

We are writing to notify you of a compromise recently reported to us by Mastercard®, where your card ending in **XXXX** may have been involved; possibly involving unauthorized transactions on your checking account. This potential compromise occurred between **October 30, 2019 and November 1, 2019**.

St. Mary's Credit Union monitors all member accounts using fraud-monitoring software that tracks card trends and spending behaviors, and will alert you or possibly deny transactions that are out of the ordinary. Due to the potential compromise, we are taking additional measures to protect you:

- **We have issued you a new card.** Your new card will arrive in the mail within the next week. If you do not receive your new card by Monday, November 18th, please contact our Member Solutions Center at 508-490-8000 or toll-free at 866-585-7628.
- **Fraud texting alerts:** if you are not signed up for our fraud texting alert system, please visit a branch or call us at the Member Solutions Center to set it up for you.
- **If we do not hear from you, we will deactivate the card ending in XXXX by 11/18/2019, due to the potential fraud.**

We ask that you monitor your account activity carefully and inform us immediately if any unauthorized transactions are posted to your account.

If you have any questions, please contact our Member Solutions Center at 508-490-8000 or toll-free at 866-585-7628, representatives are available Monday through Friday from 8:00AM to 7:00PM and Saturday from 8:00AM to 1:00PM. **Please note:** St. Mary's offices will be closed on Monday, November 11th in recognition of Veteran's Day.

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

Sincerely,

Jim Petkewich
Senior Vice President, Retail Services

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 |