

Help Us Prevent Debit/ Credit Card Fraud



Card skimming is on the rise and we need your help to minimize the loss incurred by the credit union. Skimming is the fraudulent copying of the data on a magnetic stripe by swiping a card through a magnetic stripe reading device and then transferring the data to a blank card. These skimming devices can be put over the already existing ATM card slots and payment terminals. In addition, handheld skimming devices have known to be used at retail stores and restaurants. The cloned cards are then used to make purchases from your account. Although you are not liable for the fraudulent purchases, the credit union will likely incur the loss.

Here are some ways to protect yourself and the credit union from possible fraud:

- Use ATMs you're familiar with so any changes will be more apparent; for example, a device over the card reader or a note telling you to swipe your card through a reader other than the one in the machine
- Conduct ATM transactions during the day – most ATM crime occurs in the evening
- Watch for "shoulder surfers" who watch you enter your pin or people sitting in cars nearby monitoring the ATM activity. Be wary of people who try to "help" you at an ATM
- Look at the ATM or retail card reader before using it. If it doesn't look right or is loose, don't use it.
- Stand close to the ATM or payment terminal and shield the keypad with your hand when keying in your PIN (you may wish to use the knuckle of your middle finger to key in the PIN)
- Know where the security cameras are located. While many ATMs and stores have cameras, they won't be positioned to record the keypad.
- Alert the credit union of anything that seems suspicious or strange about the ATM machine
- Regularly check your account through our Home Banking site and your statements for discrepancies and report it to the credit union immediately