

# Security Alert: Debit and Credit Card Skimmers

In an ongoing effort to keep our members safe, we would like to share some information about credit and debit cards skimming devices. Please note that we have no current evidence of cards being compromised; this is an informational security alert. Friendly reminder: Always keep an eye on your card statements to look for unauthorized charges! And as always, you can use your RFCU contactless (tap-to-pay) card for added security.

What is card skimming?

Card skimming is a method thieves use to collect data from your credit or debit card magnetic strip at the time you use it. Point-of-purchase machines, such as gas pumps, ATMs, and transit ticket dispensers, are most susceptible to skimming devices.

As thieves become savvier, it's important for you to keep your eyes open when using your credit or debit card. Follow these guidelines every time you use your card:

Tips to Avoid Being Skimmed

1. Do a quick scan. Before using any machine, take a look to make sure it hasn't been tampered with. If the card reader seems loose, crooked, or damaged, don't insert or swipe your card. If there is another machine nearby (such as two ATM machines next to each other) compare them to see if there are obvious differences.
2. Be wary of non-bank ATMs. FICO reports that 60% of skimming occurs at privately-owned ATMs.
3. Check the keypad. If the numbers are hard to press or feel thick, it might have a false keypad installed and you should move on to the next machine.
4. Block your PIN. Cover the keypad with your other hand in case a camera is recording your number.
5. Use a mobile wallet. An alternative to swiping your card is paying by mobile wallet including Apple Pay, Samsung Pay, or Google Pay. This form of payment is secure because your credit card information is tokenized and rendered useless if a thief were to get a hold of it.
6. Pay inside. If your local gas station hasn't yet updated their pumps to accept mobile wallets or you aren't sure if the machine is safe, go inside the service station to pay.
7. Always use machines that are in public view with security cameras – these machines are less likely to be tampered with.
8. Monitor your account regularly. Check your account using online and mobile banking. This way, if anything were to happen, you can catch it immediately and report it to RFCU.

9. Set up notifications with RFCU by downloading the RFCU Cards app from your app store. While fraud is not 100% preventable, catching issues immediately will save you a lot of headaches. At RFCU you are automatically enrolled in text alerts that can help prevent fraudulent transactions on your credit and debit cards. If a suspicious transaction occurs, RFCU will send a text to your mobile phone asking you to verify the transaction.

10. Above all, trust your instincts. If you suspect foul play, or if you're in doubt about the authenticity of a machine, use a different machine or payment method.