

What is Debit Card Skimming?

Skimming occurs when the information contained on your debit card is stolen and then counterfeited and used to obtain funds from your account without your authorization. Card reading devices are used to obtain the electronic data from the magnetic stripe on your card, and hidden cameras or false personal identification number (PIN) pads are used to obtain your personal access code.

How does it happen?

1. At an ATM, a card reader is placed on the ATM itself, or the entrance door to the ATM. A hidden pin-hole camera is used to capture your PIN.
2. At point-of-sale (POS) terminals, the merchant usually swipes your card in the legitimate POS terminal, and then swipes your card a second time in a card reading device. The three ways that your PIN can be obtained is by a video camera, someone watching you, or a false PIN pad.

How can you protect yourself?

1. Keep your card in a safe place and never lend it to anyone.
2. Protect your PIN; it is the key security feature on your debit card. Use your hand, body or wallet to shield your PIN when using an ATM or POS terminal.
3. Always memorize your PIN. Never write it down, and don't use a number that would be easily identified. (ie: date of birth, address or phone number)
4. Changing your PIN regularly will help reduce the risk of card skimming.
5. Never disclose your PIN. No one from a financial institution, police service, or business should ever ask for your PIN.
6. Look for physical alterations on ATM and POS terminals. If they look suspicious do not use them and inform the financial institution or merchant immediately.
7. Keep an eye on your debit card when conducting a transaction; only allow your card to be swiped once. Whenever possible, swipe the card yourself and remember to take your card and the transaction record with you when you leave.
8. Be alert. Make sure no one is looking over your shoulder. If someone is watching you or makes you feel uncomfortable, cancel the transaction and use a different machine.
9. Always conduct your ATM transactions when and where you feel most secure. If you feel uncomfortable using a specific machine, use it later or go to another location.
10. Check your bank account regularly and compare your transaction records against your financial statements. If you detect any unusual account activity, contact your branch immediately.

What should I do if I suspect fraud?

Immediately contact your Community Savings branch or call 1.888.888.8792 if:

- You think your debit card has been compromised due to skimming fraud,
- Your debit card is lost or stolen, or
- Your card is retained by an ATM.