

What is Skimming?

A method used by criminals to capture debit or credit card data from the magnetic stripe on the back of an ATM card. However, in order to commit fraud the card data and PIN information are both needed.

What is PIN Capturing?

A method used by criminals to obtain your credit or debit card's PIN information. Methods include social engineering (human interaction) techniques, strategically placed cameras, and/or false keypads to capture PIN information. Many skimming attacks use a combination of technical and social engineering techniques such as the 'good Samaritan' or 'friendly and helpful' passerby who may offer to enter your PIN for you. NEVER give your PIN to anyone!

Remember the following to keep yourself safe when using any ATM, Kiosk or automatic payment system:

- **Cover Up!** Shield your PIN entry on the ATM or Kiosk keypad with your spare hand when entering information. By protecting your PIN, criminals won't have access to your account if your card information is compromised.
- **Stand close** to the ATM and use your body as a shield as extra security to protect your card and PIN.
- Do not accept assistance and guidance or allow just anyone to interfere with your transaction – fraudsters sometimes pose as credit union or bank officials and offer assistance or interfere with your transaction.
- **Report** any unusual appearance or any difficulty using an ATM or Kiosk immediately.
- If you suspect that a skimming device is attached to an ATM or Kiosk, DO NOT attempt to remove it or tamper with it in any way. The criminals who engage in this type of fraudulent activity are known to become violent as they are typically not far away from the scene observing.
- **Be vigilant** in reviewing your account transactions frequently for irregularities or unidentifiable charges or transactions.
- [Sign up for eAlerts](#) so you know right away if there's fraudulent activity on your accounts.
- Only insert your card when the ATM prompts you to do so – fraudsters may jam ATMs to create confusion with customers.
- Don't allow anyone to call you back to the ATM or KIOSK after transacting, requesting you to insert your card again – fraudsters use this technique to confuse customers who've already finalized their transactions and are busy walking away.
- **Be observant** of your surroundings when transacting at the ATM. Leave the ATM immediately if you feel unsafe or when suspicious people are loitering in the area.

- Use ATMs you are familiar with and avoid using ATMs in secluded areas or late at night. Choose ATMs in high traffic areas that are well lit.
- Never force your card into an ATM slot.
- If your card is trapped or captured by an ATM, do not leave the ATM. Call the debit card lost & stolen number immediately to cancel the card before leaving the ATM.
- Do not accept an offer to use someone else's phone when phoning your bank to cancel your card.