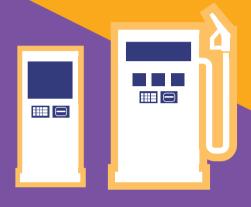
# SIMPLE STEPS

**can keep you safer** at the ATM and fuel pump.



Card skimming occurs when a card's magnetic stripe information is copied at an ATM or fuel dispenser, through an electronic device or software.

That card's information is then cloned / rewritten onto a new card.

## KEEP YOURSELF SKIM SAFE WITH 5 SIMPLE STEPS

- 1. Set online and mobile banking fraud alerts.
- 2. Tug the card reader. Is it loose?
- 3. Examine your surroundings.
- 4. Protect your PIN; cover it with your hand.
- 5. Scan for security tape seal on pump.

#### ATM SAFETY



Use an ATM in a well-lit area.

Prior to inserting your card: Wiggle the card reader. If you notice something suspicious call 911.





Cover the PIN pad with your hand when entering your PIN to guard against hidden cameras.

#### **FUEL PUMP SAFETY**

Use a pump closest to and facing the store.





Prior to inserting your card: Wiggle the card reader. If you notice something suspicious call 911.

Check that security seal tape is intact. If seal is broke, let store know and pay inside.



### SET SECURITY ALERTS FOR ADDED SAFETY



Set your online and mobile banking fraud security alerts. Closely monitor your accounts and call your financial institution if you suspect fraud.

