

# FRAUD ALERT

## Watch Out for “Skimming”

Last week, the Fraud Prevention Task Force received a report of skimming devices being used in the St. Louis area. “Skimming” occurs when a criminal places an additional card reading device onto the card reader of an ATM, gas station pump or retail store. The skimming device is difficult to detect and often matches the valid card reader. It electronically captures the card’s data, which allows the scammer to create a copy of the victim’s credit, debit or ATM card. The card’s PIN number is recorded simultaneously by either a hidden camera or the fraudster himself. Skimming is also committed by dishonest food servers who carry portable devices to record the card data of customers.

The citizen in this reported case used a debit card at several locations before discovering unauthorized purchases after checking her bank account online. She immediately notified her bank. Fortunately, the bank had also picked up on the suspicious transactions and blocked the card after three successful purchases totaling \$150. The criminals then failed in ten other attempts to use her card. Sadly, this citizen is one of many who unknowingly fall victim to this fraud each year: Bankrate.com estimates \$1 billion is stolen annually from ATM machines through skimming.

### **The FBI, Federal Trade Commission and other agencies recommend consumers take these precautions to avoid being “skimmed”:**

- Inspect the ATM, gas pump, or credit card reader before using it. If anything looks loose, bent or damaged (scratched, tape residue on it), don’t use it. Gently tug on the device to see if it is loose.
- When entering your PIN, block the keypad with your other hand to prevent hidden cameras from recording the number.
- Use ATM machines in well-lit, public areas. Inside locations are less prone to skimming.
- Don’t use an ATM with unusual signage or instructions, such as telling you to enter your PIN twice to complete the transaction
- If you give your card to a store clerk or restaurant server to swipe, watch carefully to insure your card is not swiped twice, especially on two different devices.
- Check your bank accounts frequently to promptly detect unauthorized transactions.
- Notify the police and bank if you suspect a fake device is being used.

For more information, go to the websites of the FBI ([www.fbi.gov](http://www.fbi.gov)) or Federal Trade Commission ([www.ftc.gov](http://www.ftc.gov)) and type “skimming” into their search bars. Both sites are valuable resources for information on this as well as other frauds and scams.



*To Pursue Justice for All Citizens Within the Highest  
Standards of Ethical Behavior and Professionalism*

**Fraud Assistance Hotline:  
(314) 612-1412**