Fraud Alert!

Financial Fraud Update
Card Skimming

- Protect yourself
- Know the facts
- How it happens
- Safety tips

Recently, security experts have reported an alarming increase in the incidence in account fraud using an older scam — card skimming. Card skimming is the illegal collection of your personal and account information from the magnetic stripe of a credit, debit or ATM card.

How does skimming happen

Criminals use a variety of "skimming" methods to steal information from the magnetic stripe on your cards. Sometimes a look-alike card reader face plate is used or sometimes a small recorder is attached to or placed inside the card reader. These are the most common methods.
Fact: This fraud can happen any place where financial transactions are initiated using outdated card readers — retail stores, restaurants, gas station pumps or other businesses.

Smart cards and security improvements

There are new ATM machines, new card readers, new micro-chip cards, new payment protocols and certification with the investment of billions of dollars to make it all happen. Yet, while smart cards with chip technology offer unmatched security, the full implementation of the technology is still not complete.

What's the situation today

- Point-of-sale (POS) terminals at merchant locations needed replacement or an upgrade then re-certification to accept payments using the micro-chip cards. Most merchants have updated card readers to accept the chip technology.
- Automated fuel dispensers better known as gas pumps are not required to have the new chip technology and payment certification standards in place until the fall of 2020.

- ATM machines have been re-certified and employ the new technology — only a small number of independent ATMs in remote locations still use the outdated "magnetic stripe" technology.

It is easy to understand that, while the future will be safer using smart cards, the danger of card skimming today is real.

Follow these tips to increase your safety

Fortunately, there are some common-sense protections card users can take to protect themselves from "skimming" scams.

- **Stick with what you know**—Use ATMs that are familiar to you (such as your financial institution) and share your card only with reputable merchants.
- **Use common sense**—Look at the machine. If it looks tampered with, it likely is. Report it to the owner and go to another location rather than risk using it!
- **Check your balances regularly**—By keeping a watchful eye, criminals can be stopped sooner.
- **Report any suspicious activity** or unauthorized purchases immediately. This step limits your potential financial liability (information on consumer liabilities and protections is available at www.ftc.gov).
- **Protect your PIN**—Shield the keypad when you enter your PIN, since skimmers sometimes use cameras to steal your password information

Don't let this fraud happen to you! Protect yourself today and tomorrow. Know the facts.

Additional Resources

- Federal Trade Commission
  http://www.ftc.gov
- U.S. Treasury Department
  http://www.treasury.gov
- Federal Reserve Board
  http://www.federalreserve.gov