

---

Fraud Alert!

## Credit, Debit & ATM Card Skimming



---

Full implementation of credit, debit and ATM cards with micro-chip technology promises to help end card skimming. Until then, protect yourself against this resurgence of an old scam.

Micro-chip card technology promises to provide unparalleled protection to card-users wherever and whenever they use them. And yet, security experts are reporting a shocking rise in an old card scam—**skimming**—with a 546% increase in one report!

### ■ Why the increase in an old scam?

---

Skimming is when personal data is illegally collected from the *magnetic stripe* of a credit, debit or ATM card. This data is then used to make purchases or withdraw cash. Skimming works by replacing a card reader with a look-alike skimming device at an ATM or POS (point-of-sale) terminal. It can happen at ATMs, retail stores, restaurants, taxis or other businesses where a criminal has fitted the card reader with a skimmer.

### ■ Why is this happening...and how can I stop it?

---

The “why” is relatively easy: *criminal opportunity*. While chip cards potentially offer unmatched security, the implementation of the technology is still a work in progress. A few statistics make the magnitude of the job quite clear:

- 15 million POS terminals needed upgrading to accept chip cards.
- Many merchant locations are still unprepared to accept the technology.
- 1.2 billion cards needed to be upgraded with chip technology.
- 425,000 ATM machines reprogrammed or replaced to receive the chip technology.

So it is easy to see that, while the future appears safer, the danger today is real.

### ■ Tips to increase your safety

---

Here are some common sense practices 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’s) and use your card only with reputable merchants.
- **Use common sense.** Look at the machine. If it looks tampered with, it likely is. Go to another location rather than risking it!

- **Check your balances regularly.** By keeping a watchful eye, criminals can be stopped sooner.
- **Report any suspicious activity** or unauthorized purchases immediately to your card-issuer to limit your financial liability (information on consumer liabilities is available at **[www.ftc.gov](http://www.ftc.gov)**).
- **Protect your PIN.** Shield the keypad when you enter your PIN, since skimmers sometimes use cameras to steal your information.

Certainly, no one wants their money stolen, but more harmful to many is the loss of their financial security that goes along with identity theft. Identity theft and its aftermath can take years to recover from.

Don't let it happen to you! Protect yourself today. And remember, your financial institution is always there to help you understand the threats to your financial security.

#### ■ **Additional resources**

---

- Federal Trade Commission  
**<http://www.ftc.gov>**
- U.S. Treasury Department  
**<http://www.treasury.gov>**
- Federal Reserve Board  
**<http://www.federalreserve.gov>**
- Consumer Financial Protection Bureau  
**<http://www.consumerfinance.gov>**