

## **More prevention tips**

### **Know who you're dealing with**

Scammers often pretend to be someone you trust, like a government official, a family member, a charity or company you do business with. Check with a state or local consumer protection agency and the Better Business Bureau (BBB) to see if the seller, charity, company, or organization is credible. Be especially wary if the entity is unfamiliar to you. Do not send money or give out personal information in response to an unexpected request.

### **Don't believe your caller ID**

Scammers may pose as government officials, law enforcement officers or bank employees to steal your personal information. Scammers use local numbers to trick you into answering when they call. The number you see on your caller ID may not be real.

### **Contact the company directly**

Don't call the phone number provided in a suspicious call, text message or email. Contact the company directly using the number from their website or a number you have used previously. Never respond to an unsolicited message.

### **Shop Safely**

A "padlock" icon located at the top of your browser window and the use of "https" in the address bar indicate a secure shopping website.

### **Always read the fine print**

Never enter your debit or credit card information to receive a free sample, free trial or free information. Some companies use free trials to sign you up for products and bill you every month until you cancel. Always read the cancellation policy before agreeing to a free trial.

## Skimming Devices

Skimming devices are small devices that scan a credit/debit card and store the information contained in the magnetic strip. Skimming devices are used as a means of electronically capturing a victim's personal information used by identity thieves. Skimming can take place during a legitimate transaction at a business. Skimming devices are most common on gas pumps and ATMs.

How to protect yourself against skimmers

- Use ATM's in public, well lighted areas
- Check ATM for overlay skimmers – grab the card reader to make sure it is secure.
- Cover your hand when entering your pin number to protect your pin
- Use gas pumps closest to or in view of the store
- Look for tamper proof security tape over the lock on the gas pump
- Use credit instead of debit on gas pumps to prevent your pin number from being recorded