What is Identity Theft?
Identity theft occurs when someone uses your name, address, Social Security number (SSN), bank or credit card account number, or other identifying information without your knowledge to commit fraud or other crimes.

Credit Card And ATM Fraud
Before Jay Foley inserts his bank card into an ATM slot, he sticks his finger in. Then he wiggles it. "If any portion of it wiggles with my pinky, I walk away, because the odds are somebody has slapped a skimmer on the front," says Foley, the executive director of the Identity Theft Resource Center in San Diego. "That applies to any kind of payment slot you might run across, such as gas station pumps. Those are favorite places for thieves to work now."
A skimmer is a device that reads and records all the account information stored electronically on the magnetic strip of an ATM card. With a little light mechanical tampering, thieves can "harvest" your account details and PIN number in seconds, then use them to either produce or "clone" card or to simply shop online until your account runs dry.
"The number of victims we get from debit fraud or ATM fraud is growing every year, and is growing significantly." Foley says.
Thieves have also been known to purchase bogus ATM machines and place them in remote areas or put an out of order sign on a working ATM to direct traffic to their nearby bogus ATM. They have also been known to put up a machine that says, "We will clean the mag stripe on your debit cards. Just insert it here, and it will improve the transaction process," Foley says. "What you are doing at that point is plugging it into a skimmer."

Watch For Signs Of Foul Play
When choosing an ATM, keep the following things in mind:
Use a familiar and trusted ATM, preferably one attached to your bank. Avoid using ATMS in unfamiliar or remote locations, or around suspicious persons.
Check the card slot, keyboard and machine for signs of tampering. Do not use the machine if the card slot jiggles, the keyboard has an overlay or anything else seems suspect.
Look for security cameras on the machine and in the vicinity. If they appear suspicious, do not use the ATM.
Avoid ATMs with signs or messages affixed to them. Banks and legitimate ATM owners do not direct customers to another machine with signs attached to the machine itself.

Smart Ways To Avoid ATM Fraud
Always safeguard your information by following these steps when using an ATM:
Maintain a safe distance from others in line. Do not allow anyone to distract you or offer assistance.
Have your card out of your purse or wallet and ready for use.
Stand close to the screen and shield your keystrokes from cameras and others waiting in line by using the knuckles of your middle finger to key in your PIN.
If you think your ATM is not working properly, press cancel, remove your card, and report the machine to your financial institution.
Secure your cash and card, and make sure the transaction is completed and the screen is clear before leaving the ATM.
Keep your printed receipt to compare against your bank statement.
This article was reported and written by Jay MacDonald for Bankrate.com

Protecting Your Identity

The number of Americans who have experienced identity theft has surpassed 27 million, with the incidence rate increasing every year. Substantial measures are in place at USFCU to protect your identity and your accounts against theft and fraud. For example, stringent credit union privacy policies protect your personal information. Password protection for online transactions helps assure online security. When using our online services, you develop a password that only you know. Encryption of online transactions converts your information into secure code, protecting you against hackers.

How to Guard Against ID Theft

Maximum security is possible *only with your help.* Here's what you can do to stop these crimes before they happen:

1. **Do not give out financial information** such as checking and credit card numbers, or your Social Security number, unless you initiated the transaction/conversation.
2. **Shred any pre-approved credit card offers, financial statements, and receipts** before you throw them out.
3. **Report lost or stolen checks immediately.**
4. **Notify USFCU of suspicious phone inquiries** such as those asking for account information to "verify a statement or fraud activity" or "award a prize."
5. **Be creative when you select a password.** Don't be obvious like using the last four digits of your social security number, phone number, address, birth date or any format that could easily be decoded by thieves.
6. **Memorize all passwords and PIN numbers** so no one can see them in writing.
7. **Remove mail promptly from your mailbox.** Identity thieves raid mailboxes for credit card offers and financial statements. Put outgoing mail into a secure, official Postal Service collection box.
8. **Keep a list or photocopies** of all information & cards you carry in your wallet or purse. Store this information in a secure location.
9. **Keep your birth certificate and social security card in a safe deposit box.** Carry those items with you only on the days you need them.
10. **Review your credit report each year**. If someone is applying for credit in your name and you haven't noticed any warning signs, a copy of your credit report may help point this out. You can obtain a free credit report once a year from each of the credit reporting agencies – Experian, Equifax, and Trans Union. **Online at www.annualcreditreport.com or toll free at 877.322.8228**.

What to do if you are a Victim

1. Contact your credit card company, USFCU, and any other financial institutions you may have and close your accounts. The FBI suggests that you put passwords (not your mother's maiden name) on any new accounts you open.
2. Call the three major credit bureaus (numbers listed below) to tell them your identity has been stolen. Request that a "fraud alert" be placed on your file and that no new credit be granted without your approval.

   EQUIFAX: 800-525-6285
   EXPERIAN: 888-397-3742
   TRANS UNION: 800-680-7289
3. Call the Social Security Fraud Hotline: 800-269-0271
4. Contact the Federal Trade Commission (FTC) theft hotline: 877-438-4338 or www.consumer.gov/idtheft

5. You should not only file a report with the police, but also get a copy of the report in case you need proof of the crime later for credit card companies, etc.