Identity Theft Tips

Credit Union Policy

We will NEVER ask you to confirm you personal information using a link in an email.
When you receive a legitimate email from us we will advise you to access our website and Internet Banking by using your own bookmarks or favorites.

Identity Theft Warning Signs

- Fraudulent charges on your credit card statement
- Credit card or financial statements don't arrive
- Bills arrive for goods or services you didn't request
- Phone Calls from creditors
- Suddenly denied credit

How To Guard Against Identity Theft

- Guard your social security number. Don not give out your PIN or credit card numbers over the phone unless you initiated the transaction.
- Be very careful with receipts. Make sure you have them when you leave the store or ATM and do not throw them into public trash cans.
- Destroy pre-approved credit card offers before you throw them out. A home shredder is the best thing to use on financial statements, receipts and old cancelled checks that you are discarding.
- Commit all passwords and PIN numbers to memory so no one can see them in writing.
- Limit the number I.D. and credit cards that you carry. If they are stolen, you'll have fewer to replace.
- Keep your birth certificate and social security card in a safe deposit box. Carry these items with you only on the days that you need them.
- 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. Online at www.AnnualCreditReport.com or 1-877-322-8228.

Help Keep Online Transactions Secure

- Avoid sending sensitive information, such as account numbers through UNSECURED email.
- Passwords or PIN numbers should be used when accessing an account online.
- General security over your personal computer such as virus protection and physical access controls should be used and updated regularly.

Phishing

- Phishing attacks are "spoofed" e-mails and fraudulent web sites designed to fool recipients into divulging personal financial data such as credit card numbers, account user names and passwords, social security numbers, etc. By hijacking the trusted brands of well-known financial institutions, online retailers and credit card companies, phisheres are able to convince up to 5% of recipients to respond to them.

How to Avoid Phishing Scams

- Be suspicious of any e-mail with urgent requests for personal financial information.
- Don't use the links in an e-mail to get to any web page, if you suspect the message might not be authentic.
- Always ensure that you are using a secure website when submitting credit card or other sensitive information via your web browser.
- Regularly log into your online accounts and check your financial institution credit and debit card statements to make sure that all transactions are legitimate.
- Make sure that your browser is up to date and security patches applied.

What To Do If You Are A Victim

1. Contact your credit card company and your financial institution 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 shown 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,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.