Protecting Yourself from Fraud
Victim Information Resource

Protecting Against Check Scams

Check Scams can take several different forms, including:

- Buying something you are selling in an advertisement;
- Paying you to work at home;
- Giving you an "advance" on a sweepstakes or lottery you have won;
- Giving you money for agreeing to transfer money in a foreign country to your bank account for safekeeping.

There is **no legitimate reason** for anyone who is giving you money to ask you to wire funds back to them or to someone else.

Do Not Deposit the Check. If you think you might have received a fake check, don't deposit it…report it. Bring the information to the bank and ask for assistance.

Report Check Scams to:
National Consumers League's
National Fraud Information Center
www.fraud.org or call (800) 876-7060

How to Protect Your Identity

First Line of Defense: YOU!

Be aggressive about your security. Here are some ideas of ways to protect your identity from identity thieves.

- **Don't give out or confirm personal information** over the phone or on-line. You may be a victim of a Phishing Scam. If it is a company you know, call them yourself or go to their Web page yourself rather than clicking on the link in the e-message.
- **Remember… a REAL BANK, Credit Card Company, etc. never sends e-mails asking for your account information.**
- **Shred mail** you receive that you choose not to use. Especially pre-approved credit offers and any document that has your name or personal, identifying information on it.

- **Outgoing mail** should not be left in a mailbox with the flag up. Place in a USPS box instead.
- **Take advantage of Opt Out Offers**
    - ***Reduce the number of pre-approved credit offers*** by registering to have your name removed from the marketing lists of the three credit bureaus. Go to www.optoutpresscreen.com or call 1-888-567-8688.
    - ***Reduce the number of phone call solicitations*** by registering on the National Do Not Call Register maintained by the Fair Trade Commission at www.donotcall.gov or 1-888-382-1222. Call from your home phone.
- **Order a copy of your credit report** every 12 months and review it for unauthorized use of your credit. Call 1-877-322-8228, go to www.AnnualCreditReport.com or go to CSB's web site and click on the link that site. Under the Fair and Accurate Credit Transactions Act of 2003, consumers are entitled to one free report per year from each reporting agency. Other companies who advertise credit report retrieval and monitoring typically charge a fee.
- **Closely monitor** monthly credit card and bank statements for unauthorized activity. If you don't receive a regular bill or statement on schedule, call the company and find out why. Someone may have falsely changed your mailing address.
- **Cancel and destroy all cards** that have had little or no activity for the last six months. When you close the account with a creditor, ask for confirmation in writing.
- **Don't carry items** in your wallet/purse that are not used regularly (e.g. birth certificate, SS cards, passports, excess credit cards, PINs). Don't carry anything that will help the criminal steal your identity.
- **Don't leave sensitive mail** for postal carriers to pick up – take important mail items directly to the post office or a neighborhood drop box.
- **Lock up** your checkbook, extra checks, cards, and investment records.
- **Watch for "shoulder surfers"** when using ATM and Point of Sale machines.
- **Check Orders** should not have pre-printed drivers' license or phone numbers on the checks. Use first and middle name initials rather than full names. Order from the bank rather than independent vendors.
- **Be creative in selecting a PIN and passwords.** Don't use common information, like your date of birth, which can easily be found.
- **Report Lost or Stolen Checks** immediately!
- **Install Security Software** on your home computer and make sure to update it at least weekly.

What to Do If You Become a Victim

REACT QUICKLY!

#1 Rule: ***Keep accurate records of the contacts you make for each step. You will need this information.***

- **Call the fraud unit of the 3 credit reporting companies.** Report the theft of your credit cards or numbers. Ask that the accounts be flagged. Have them add a victim's statement to your account.
- **Contact your credit card issuers.** Get replacement cards with new account numbers. Make sure old accounts are processed as "account closed at consumers' request."
- In addition to contacting individual card issuers directly, report to:

VISA USA:
1-800-235-5520
Mastercard International:
1-800-627-8327
American Express:
1-800-843-2273
Discover:
1-800-347-2683

- Monitor future credit card statement for unauthorized transactions.
- Report crime to your local police and **IMMEDIATELY** obtain a copy of the report.
- Report to the U.S. Secret Service.

Email: 419.fcd@usss.treas.gov.
Fax: (202) 406-5031
Mail: U.S. Secret Service
Financial Crimes Division
950 H St. Suite 5330, NW,
Washington D.C. 20373-5802 (Attn: 419)

- Notify your bank of the theft. Close accounts involved and obtain new account numbers and checks. If new accounts were set up, notify the banks and notify check verification companies immediately. If ATM cards are stolen, get a new card, account number, and password.
- When selecting passwords, avoid commonly used names and numbers for passwords.