Protecting Yourself Against Fraud

Protecting Your Personal Information

- Carry only necessary identification. Do not carry your social security card with you.
- Be cautious when providing your Social Security Number. It's okay to ask whether it is needed for the application or transaction.
- Check your credit report annually at a minimum.
- Never provide personal information over the phone or internet unless you have initiated the contact and have confirmed the business or person's identity.
- Avoid leaving any personal information in your car.
- Shred unnecessary documents and eliminate as many paper documents containing your personal information as possible.

Protecting Your Bank Accounts

- Use online services to monitor your bank accounts regularly.
- Receive your paychecks, dividends and other reoccurring deposits directly into your account electronically.
- Store your checks securely and know who has access to them.
- Report suspicious activity immediately (lost, stolen or unauthorized use of checks or cards).
- **Avoid writing down, carrying or sharing your online banking or card PIN (Personal Identification Number) with anyone.** Memorize it or secure it at home.
- Choose passwords or PINs that are difficult for others to guess by not using personal information within the password such as address, phone number, SSN or date of birth. It is much more secure to use random information.
- Consider different passwords for each online account. Never "lend" your debit cards to others. You are responsible for transactions initiated from a card that was lent to someone else.

Protecting Your Credit Cards

- Never provide your credit card information over the phone or internet unless you have initiated the contact and have confirmed the business or person's identity.
- Never "lend" your credit cards to others. You are responsible for transactions initiated from a card that was lent to someone else.
- Check your credit report at least annually.
- The Fair Credit Reporting Act (FACT Act) by the Federal Trade Commission allows you to ask for and receive one free credit report every 12 months from each of the three major nationwide credit reporting agencies. You can get your free annual report at www.annualcreditreport.com.

Telemarketing Fraud

If you are age 60 or older—and especially if you are an older woman living alone—you may be a special target of people who sell bogus products and services by telephone. Telemarketing scams often involve offers of free prizes, low-cost vitamins and health care products, and inexpensive vacations. There are warning signs to these scams. If you hear these—or similar—"lines" from a telephone salesperson, just say "no thank you," and hang up the telephone:

- "You must act now, or the offer won't be good."
- "You've won a free gift, vacation, or prize." But you have to pay for "postage and handling" or other charges.
- "You must send money, give a credit card or bank account number, or have a check picked up by courier." You may hear this before you have had a chance to consider the offer carefully.
- "You can't afford to miss this high-profit, no-risk offer."

Tips for Avoiding Telemarketing Fraud:

It's very difficult to get your money back if you've been cheated over the telephone. Before you buy anything by telephone, remember:

- Don't buy from an unfamiliar company. Legitimate businesses understand that you want more information about their company and are happy to comply.
- Always ask for and wait until you receive written material about any offer or charity. If you get brochures about costly investments, ask someone whose financial advice you trust to review them. But, unfortunately, beware—not everything written down is true.
- Always check out unfamiliar companies with your local consumer protection agency, Better Business Bureau, state attorney general, the National Fraud Information Center,

or other watchdog groups. Unfortunately, not all bad businesses can be identified through these organizations.

- Obtain a salesperson's name, business identity, telephone number, street address, mailing address, and business license number before you transact business. Some con artists give out false names, telephone numbers, addresses, and business license numbers. Verify the accuracy of these items.
- Don't pay in advance for services. Pay services only after they are delivered.
- Always take your time making a decision. Legitimate companies won't pressure you to make a snap decision.
- Don't pay for a "free prize." If a caller tells you the payment is for taxes, he or she is violating federal law.
- Before you receive your next sales pitch, decide what your limits are—the kinds of financial information you will and won't give out on the telephone.
- Be sure to talk over big investments offered by telephone salespeople with a trusted friend, family member, or financial advisor. It's never rude to wait and think about an offer.
- Never respond to an offer you don't understand thoroughly.
- **Never send money or give out personal information such as credit card numbers and expiration dates, bank account numbers, dates of birth, or social security numbers to unfamiliar companies or unknown persons.**
- Be aware that your personal information is often brokered to telemarketers through third parties.
- If you have been victimized once, be wary of persons who call offering to help you recover your losses for a fee paid in advance.
- If you have information about a fraud, report it to state, local, or federal law enforcement agencies.