Common Scams

- **Selling Goods.** The consumer sells goods in the marketplace, for example, over the internet. A buyer sends the consumer a check for the agreed-upon price, and the consumer ships the goods to the buyer.
- **Excess of Purchase Price.** This pattern is similar to the one described above. However, the buyer sends the consumer a cashier's check for more than the purchase price and asks the consumer to wire the excess to a third party, often in a foreign country.
- **Unexpected Windfall.** The consumer receives a letter stating that the consumer has the right to receive a substantial sum of money. For example, the letter may state that the consumer has won a foreign lottery or is the beneficiary of someone's estate. The letter will explain that the consumer must pay a processing fee/transfer tax or fee before receiving the money, but a cashier's check will be enclosed to cover that fee. The letter will ask the consumer to deposit the check into an account and wire the fee to a third party, usually in a foreign country.
- **Mystery Shopping.** The consumer receives a letter stating that he or she has been chosen to act as a mystery shopper. The letter includes a cashier's check, and the consumer is told to deposit the check into his or her account. The consumer is told to use a portion of these funds to purchase merchandise at designated merchants and to transfer the remainder of the funds to a third party using a designated wire service company.

In each of these scenarios, the consumer believes that the cashier's check is valid and deposits the check into an account. After the financial institution makes the funds available to the consumer, the consumer sends goods or, where requested, funds to the third party. Some time later, the check is returned unpaid because the check is discovered to be fraudulent. The financial institution then reverses the credit to the consumer's account. As a result of this check fraud, the consumer suffers a loss of the goods sold, the funds wired or both.

How can you protect yourself?

Of course, the best way to protect yourself is to know the person you're dealing with. Ask yourself:

- Do I know the person?
- What is the likelihood that they are who they say they are?
- Are they telling me a story or making excuses?
- Are they acting with a sense of urgency?
- Are they offering me a deal that is too good to be true (like paying more than the asking price)?
- Are you being asked to wire money to someone in a foreign country?

If you're not comfortable with the answers you get, it could be a scam and you should refrain from going forward with the transaction.

When accepting a cashier's check or other official instrument, consider:

- Whether the transaction is one that might attract a fraudster.
- Contacting the issuing financial institution to verify that the check is authentic. Be sure to use a phone number you know to be legitimate; don't assume the number on the check is correct.
- Not going through with the transaction if you can't authenticate the check.
- Not releasing the goods until the check has cleared.
- Contacting us if you suspect an at-risk situation, maybe we can help.

Identity Theft & Fraud Detection

EDGAR COUNTY BANK

www.edgarcountybank.com

Paris • Brocton • Kansas • Ashmore

PROSPECT BANK

A DIVISION OF EDGAR COUNTY BANK & TRUST CO.

www.theprospectbank.com

Champaign • Gilman • Watseka

FIGHTING BACK AGAINST IDENTITY THEFT

EQUAL HOUSING LENDER

MEMBER FDIC

Identity theft is a serious crime. It occurs when your personal information is stolen and used without your knowledge to commit fraud or other crimes. Identity theft can cost you time and money. It can destroy your credit and ruin your good name.

Deter identity thieves by safeguarding your information.

- Shred financial documents and paperwork with personal information before you discard them.
- Protect your Social Security number. Don't carry your Social Security card in your wallet or write your Social Security number on a check. Give it out only if absolutely necessary or ask to use another identifier.
- Don't give out personal information on the phone, through the mail, or over the Internet unless you know who you are dealing with.
- Never click on links sent in unsolicited emails; instead, type in a web address you know. Use firewalls, anti-spyware, and anti-virus software to protect your home computer; keep them up-to-date. Visit OnGuardOnline.gov for more information.
- Don't use an obvious password like your birth date, your mother's maiden name, or the last four digits of your Social Security number.
- Keep your personal information in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your house.

Detect suspicious activity by routinely monitoring your financial accounts and billing statements.

Be alert to signs that require immediate attention:

- Bills that do not arrive as expected
- Unexpected credit cards or account statements
- Denials of credit for no apparent reason
- Calls or letters about purchases you did not make

Inspect:

- Your credit report. Credit reports contain information about you, including what accounts you have and your bill paying history.
- The law requires the major nationwide consumer reporting companies—Equifax, Experian, and TransUnion—to give you a free copy of your credit report every 12 months if you ask for it.
- Visit www.AnnualCreditReport.com or call 1-877-322-8228, a service created by these three companies, to order your free annual credit report. You also can write: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.
- If you see accounts or addresses you don't recognize or information that is inaccurate, contact the credit reporting company and the information provider. To find out how to correct errors on your credit report visit ftc.gov/idtheft.
- Your financial statements. Review financial accounts and billing statements regularly, looking for charges you did not make.

Common Ways ID Theft Happens

Skilled identity thieves use a variety of methods to steal your personal information, including:

1. Dumpster Diving. They rummage through trash looking for bills or other paper with your personal information on it.
2. Skimming. They steal credit/debit card numbers by using a special storage device when processing your card.
3. Phishing. They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.
4. Changing Your Address. They divert your billing statements to another location by completing a "change of address" form.
5. "Old-Fashioned" Stealing. They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records from their employers, or bribe employees who have access.

If you feel you have been a victim of ID Theft, contact us or visit ftc.gov/idtheft immediately for information on the next steps to take.

EQUAL HOUSING LENDER | MEMBER FDIC