Identity Theft & Fraud

Safeguarding Your Private Information

How to Identify Scams & Fraud

First Security Bank has reported a significant increase in fraud and is currently on a mission to warn the public. Fraud and scams are very active in our area in several different forms, including lottery scams, fraudulent postal money orders, internet sale scams, bank employee impersonation, and identity theft.

What is a Lottery Scam?

In a lottery scam, a consumer is sent a letter that claims that they have won a lottery or sweepstakes. They are told that taxes, handling fees, or conversion fees on the winning must be paid by wiring a large sum of money to a location outside of the United States before they can receive their jackpot. In a variation of the scheme, a consumer receives a "certified" check in the mail for a large sum of money, which they deposit into their account. The "certified" check turns out to be counterfeit and is charged back to the victim's account.

Legitimate lotteries never ask for money. They don't have to and there are not fees of any kind. The only tax you pay is paid directly to the government.

Fraudulent United States Money Orders

Another common scam is fraudulent United States Postal Money Orders. In many cases, victims are often contacted by an e-mail message or in an on-line chat room, and are deceived into accepting them as payment for items they are selling, or into cashing the money orders in `return` for a fee.

Postal officials say that the best way to identify a genuine postal money order is to look for the watermark, which, when held up to a light will reveal a repeating image of Benjamin Franklin. Genuine postal money orders also have a security strip running alongside the watermark, just to the right. If held to a light, a micro fiber strip will show the letters "USPS" along its length.

If there is any doubt on the validity of a money order, visit your local post office or call 866-459-7822.

Internet Sale Scams

An internet sale scam is a scam in which a legitimate consumer advertises an item for sale on the internet and a buyer offer the consumer's asking price. They are told that a check will be sent in advance to pay for the item. When the check is received it is for more than the agreed upon sale price. The consumer contacts the buyer who states that the bank made a mistake and askes the consumer to send back the difference via a wire transfer.

Then the money is sent back, the bank check comes back as fraud, and the full amount is deducted from the consumer's bank account. The consumer is left with a large negative account balance and the buyer cannot be located.

Bank Employee Impersonation

Bank employee impersonation is when a consumer receives a telephone call or e-mail from someone claiming to be a bank employee with a request to provide account information for verification purposes. The consumer later discovers that funds are missing from their bank account.

There is no reason for your bank to contact you and request your account number or social security number because they already have this information.

You should call or visit your financial institution to determine the legitimacy of the request before giving out ANY information.

Identity Theft

Identity Theft occurs when someone uses your personal information without your permission to commit fraud or other crimes. While you cannot control whether you will become a victim, there are steps you can take to minimize your risk.

Security and Identity Theft Tips

The Federal Trade Commission recommends the following steps:

- Order a free copy of your credit report annually
- Place passwords on your credit card, bank and phone accounts
- Secure your personal information in your home
- Don't give out personal information on the phone, through the mail or on the internet unless you have initiated the contact or are sure you know with whom you are communicating
- Treat your mail and trash carefully
- Deposit your outgoing mail in post office collection boxes or at your local post office
- Give your Social Security Card only when necessary

What to Do If You Are a Victim of Identity Theft

Take steps quickly if you have lost personal information or identification, or if it has been stolen.

- Close account immediately and place passwords on new accounts
- Cancel your driver's license or other government-issued identification and get a replacement. Ask the agency to flag your file so no one else can get identification with your name
- Place an initial fraud alert on your credit report by calling one of the three nationwide consumer reporting agencies:

  Equifax
  Mailing Address: P.O. Box 74021 Atlanta, GA 30374-0241
  Report Fraud: 800-525-6285
  Web site: https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp

  Experian
  Mailing Address: P.O. Box 949 Allen, TX 75013-9049
  Report Fraud: 888-EXPERIAN (397-3742)
  Web site: https://www.experian.com/fraud/center.html

  Trans Union
  Mailing Address: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634
  Report Fraud: 800- 680-7289
  Web site: https://www.transunion.com/fraud-victim-resource/important-contacts

Helpful Websites

Access these websites for additional information about how to protect yourself from identity theft or obtain assistance if you have been a victim.

Federal Trade Commission National Resource on Identity Theft:

http://www.consumer.gov/idtheft

Identity Theft Resource Center:

http://www.idtheftcenter.org

Free Annual Credit Report:

http://www.annualcreditreport.com