



Arm yourself with the knowledge to avoid bank fraud----the below information will guide you in keeping your money safe.

### **Identity Theft**

Be careful with your personal identification information. People who steal identities use a variety of methods:

- **Dumpster Diving**-rummaging through trash searching for personal information.
- **Skimming**-stealing credit/debit card numbers by using a special storage device when processing your card. (Sometimes found on ATM's.)
- **Phishing**-pretending to be financial institutions in an attempt to scam a customer into surrendering personal information that will be used for identity theft.
- **Changing Your Address**-Diverting billing statements to another location by completing a change of address form.
- **Old-Fashioned Stealing**-stealing wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information.
- **Pretexting**-using false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources.

### **Best Practices for Online Banking**

#### **How to use different means to help make sure the financial institution is legitimate and it's safe to transact:**

- Banks should not solicit you for passwords, account numbers, or other personal information—if you receive an email or text message requesting such; call your financial institution using the number on your statement or credit card, not the one in the email or text message.
- Access the online banking website by typing the URL ([www.wsfsbank.com](http://www.wsfsbank.com)) into the address bar, rather than any link embedded in an email.
- Always check the browser for a "lock" icon. It is important to understand that the lock signifies a secure communication channel to a website, however it does not indicate a legitimate website.
- When logging into the Online Banking system be sure to check for your personalized image. This image indicates that you are performing Online Banking on a legitimate website which has confirmed your identity.
- Check for anything that looks unfamiliar, unprofessional, or out of place to you.

**Securing your PC for online transacts:**

- Maintain active and up-to-date antivirus, spyware, and firewall protection.
- Keep your operating system (for example, Windows® XP), browser (for example, Internet Explorer), and other applications (such as RealPlayer or iTunes) updated with the latest security patches.
- Avoid transactions at wireless hot spots, Internet cafés and public Internet access points.

**Password protection:**

- Use a strong password—at least eight characters, with a combination of numbers, letters, and punctuation symbols.
- DO NOT use the same password for banking that you use for other online accounts.
- Keep your password safe—DO NOT leave your password stored in a file your computer or written on paper.
- Change your password periodically.

**Checking your statements:**

Online banking can actually help you protect your identity—log in and check your financial statements regularly. Report any unauthorized transactions immediately. Check your free annual credit report to spot accounts that may have been opened without your knowledge.

**Check Fraud**

Check fraud is one of the largest scams in the United States. It occurs when someone steals checks from your home, office or mailbox and forges your signature. Check fraud can also occur when thieves alter the amount or name on a checks that you have previously written. Always be aware of who you write check to as well as how many checks you have.

**Credit Card Fraud**

There are many ways that a person can be a victim of credit card fraud. If you card is stolen or you receive a credit card statement from a card you did not request these are warning signs of possible credit card fraud. A few ways to protect yourself include, protecting your credit cards and card numbers, don't keep PIN numbers near your cards, properly destroy all credit card receipts and statements when no longer needed, limit the number of credit cards by canceling those you don't use and cut up old cards after they expire.

### **The Phony Investigator**

In this scam, a consumer is approached by someone claiming to be a bank examiner, bank security officer, police officer, Internal Revenue Service (IRS) auditor or some other “agent” involved in an “official” review or investigation. The successful thief walks away with the cash or the confidential information that can be used to raid the consumer’s bank account. Be wary of anyone who approaches you claiming to be a government employee investigating a bank, a bank employee, or otherwise asking for access to your cash or bank records. Government agencies do not turn to bank customers to withdraw personal funds or give account information as part of an investigation. Also, in cases such as IRS audits, you’ll be notified in advance by mail.

### **Telemarketing Fraud**

With this type of fraud, people receive unsolicited phone calls or mailings with an offer of prizes, merchandise or other opportunities. People agree over the phone to give cash or bank account information up-front to take care of a supposedly minor fee or tax. Only later do people discover that the thief has taken their money. Be wary of high-pressure sales people offering prizes, goods or services that can only be delivered upon receipt of cash, a credit card number or checking account number. To avoid telemarketing fraud, buy only from a reputable telemarketing firm. Never pay a fee to receive something “free.” If you have doubts about a particular firm, contact the Better Business Bureau and/or the Federal Trade Commission to identify if any complaints have been registered against the firm. **Also be aware that no one at WSFS Bank will ever call you asking you for your credit card or account information.**

If you are looking for more detailed information on how to avoid being a victim of fraud please view the following sites:

[www.fdic.gov](http://www.fdic.gov)

[www.ftc.gov](http://www.ftc.gov)