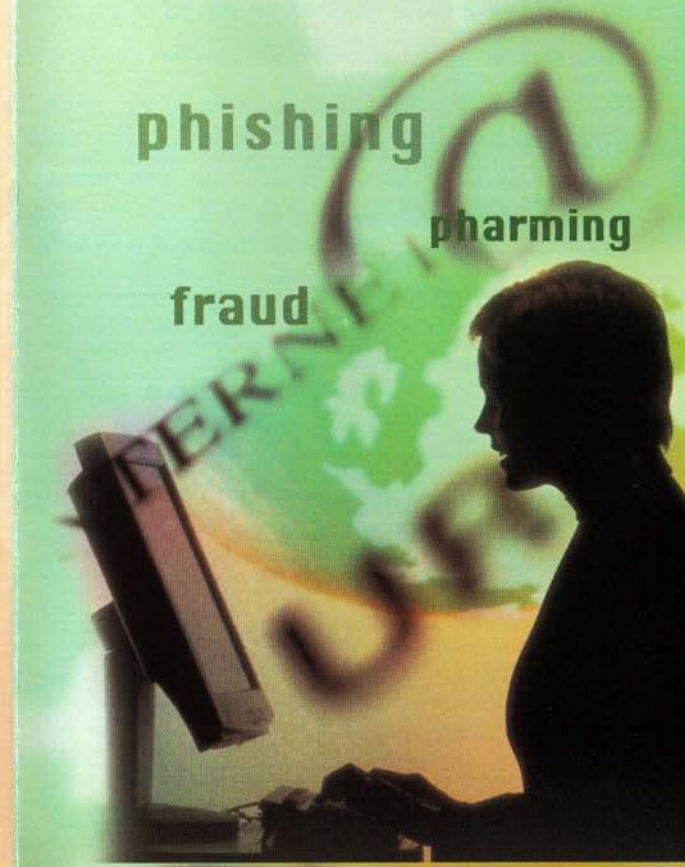
Additional Steps You Can Take to Prevent Financial Fraud

- Shred all personal and/or financial documents before disposing of them
- Destroy unused credit, ATM and debit cards
- Remove mail promptly from your mailbox
- Match receipts to monthly billing statements
- Memorize PINs, passwords and Social Security numbers
- Use longer, more complex PINs and change them periodically
- Sign all credit cards and debit cards immediately
- Notify financial institutions of address changes in advance
- Immediately report any unauthorized activity or phishing scams
- Look closely at ATMs to detect any suspicious alterations before using them
- Never use your PIN as a password

IDENTITY THEFT & FRAUD

Tips to Protect Yourself



SECURITY

Identity theft and financial fraud *are terms used to describe crimes in which someone wrongfully obtains and uses another person's personal data or financial information, typically for economic gain. This year alone, identity theft and fraud relating to electronic payments such as ATM and debit transactions and online purchases will strike millions of Americans.*

Many people do not realize how easily criminals can obtain personal data. For example, in public places criminals may listen in on your conversation or watch you from a nearby location as you punch in an account number or password. They may gain information about you by stealing unopened mail or sifting through documents that you have thrown away. In recent years, the Internet has opened the door to a variety of means for criminals to obtain your personal data.

To minimize the chances that you fall victim to identity theft and financial fraud, it is vital that you recognize the various types of fraud and learn how to protect yourself against them. The following pages will help you safeguard your identity and protect your financial assets from fraud.

IDENTITY THEFT

Identity theft occurs when your personal information is obtained and used to acquire new bank or credit card accounts, secure loans, establish utility service, get a home mortgage or even commit crime. Such information may include your address and phone number as well as more private information such as your Social Security number, bank or loan account numbers, user names and passwords, etc. One of the most popular ways criminals steal your identity is by obtaining personal information from statements or bills that you throw away. Many experts recommend that you always shred sensitive documents before disposing of them.

PHISHING

Phishing is a scheme used by fraudsters – posing as a trusted financial institution, ATM/debit network, credit-card company, online retailer or other service provider – to trick unsuspecting individuals into disclosing personal and/or financial information. Typically, you receive an unsolicited e-mail or phone call appearing to be from an organization you readily recognize asking you to verify personal and/or financial information. Many times these are organizations that may be in some way connected to your checking and/or savings account, such as your financial institution, utility company or an online payment company. To encourage immediate action, the request usually warns that an unauthorized transaction has taken place on your account, or that your service may be interrupted or shut down unless you confirm your information. If the phishing attack is in the form of an e-mail, it may use the name, logo and Web site attributes of the legitimate business.

PHARMING

Pharming uses computer software, such as crimeware, malware or spyware, to collect personal information from your computer and deliver it back to fraudsters. In pharming, consumers who are attempting to log onto a legitimate Web site are unknowingly redirected by the fraudulent software to an authentic-looking but bogus site. When the consumer enters his or her personal log-in information, the criminals capture this sensitive information and may use it for a variety of violations, including accessing your accounts and making online purchases. Since little or no participation on your part is necessary, and the redirect happens behind the scenes, pharming is extremely difficult to detect.

ATM TAMPERING

Thieves tamper with ATMs in various ways in order to steal your personal information and tap into your accounts. A perpetrator may attach a device that blocks the cash slot. When you do not receive your cash, you are likely to cancel the transaction and leave. However, the cash has already been dispensed, and the fraudster will then approach the machine and remove the device to get the money. A person may also attach a "skimming" device to the swiping mechanism, and/or a keypad overlay, that will download your account information and possibly your PIN, so that your card can later be duplicated and used for purchases and/or withdrawals.

Other Ways Criminals Get Your Personal Information

- Stealing checking/savings account statements, credit card statements, pre-approved credit offers, new checks and tax information from your mailbox
- Obtaining your credit report by posing as your landlord, employer or someone else who may have a right to such information
- Stealing wallets or purses

- Imprinting your credit or debit card, or swiping it at a skimming device, while the card is out of your sight at a restaurant or retail establishment
- Completing "change of address" forms to send your mail to another address
- Finding personal information in your home or in your trash
- Hacking into a retail store's computer system and collecting debit or credit card information such as card and PIN numbers
- Attaching a skimming device to the face of an ATM or making other alterations to the card slot or keypad to download your card information

How to Safeguard Yourself

- Do not reply to any unsolicited e-mail, pop-up message or phone call asking for personal and/or financial information. Be suspicious of anyone who contacts you with an urgent request for personal information. It is unlikely that legitimate businesses will ever engage in these practices.
- Do not click on any e-mail link if you suspect the message is fraudulent, not even to "unsubscribe." Instead, call the business using the number on the back of your card or on your monthly statement to confirm the legitimacy of the e-mail. Never send personal or financial information via e-mail.
- If you initiate an online transaction and are required to provide personal data, look for indicators that the Web site is secure, like the "https" in the URL or padlock icon. While these indicators do not ensure the security of the site or your personal data, sites without them should be avoided. You should also verify that the URL of the site you are visiting is displayed accurately in the address bar.
- Do not let your debit card out of your sight when purchasing goods and services. Although credit card information can also be skimmed, the theft of your debit card data involves greater risk because it is associated with your checking, savings or share draft account.

- Use anti-virus software, anti-spyware and a firewall, and keep them up to date. Some phishing attacks contain software that can harm your computer or track your activities on the Internet without your knowledge.
- Review account statements regularly to verify all transactions. This review should include checking, savings and credit card accounts. Frequently log into your online accounts and review all activity. Immediately report any unauthorized activity to the account provider.
- Report all phishing attacks at once. Notify the FBI by filing a complaint on their Web site at www.ifccfbi.gov and forward the e-mail to: spam@uce.gov (Federal Trade Commission).
- Change your debit card PIN periodically. Although this is probably not a step you want to take frequently, it is a good idea to change PINs periodically rather than using the same PIN year after year.
- If you have given out personal or financial information in response to a fraudulent request, report the incident to your account provider(s) as soon as possible. Keep a record of the names, account numbers and customer service numbers for all financial accounts you maintain. This way, you will have all the necessary information you need to report a theft to the appropriate account provider(s). Also, report a theft to the three major credit-reporting agencies, Experian (888-397-3742), Equifax (800-525-6285) and TransUnion (800-680-7289).
- Review your credit report every year. According to the Fair and Accurate Credit Transaction Act (FACTA) of 2003, you are entitled to one free credit report each year. In addition, you may also obtain a free credit report if you are a victim of identity theft. To request your free credit report, call 877-322-8228, log on to www.annualcreditreport.com or write Annual Credit Report Request Service at P.O. Box 105281, Atlanta, Georgia, 30348-5281.