

## What if you discover you're a victim of fraud?

- 1) Contact the fraud department of at least one of the following three major credit reporting agencies and ask that a fraud alert be placed in your credit file and for a free credit report (to be on the safe side you may wish to contact all three):
  - **Equifax**®—1-800-525-6285; P.O. Box 740241, Atlanta, GA 30374-0241
  - **Experian**®—1-888-EXPERIAN (397-3742); P.O. Box 9532, Allen, TX 75013
  - **TransUnion**®—1-800-680-7289; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790.

## Identity Fraud

- 2) Close all accounts that are or may be affected by the identity theft.

Also, regarding any checking accounts thus closed, contact the following major check verification companies and ask that retailers using their databases not accept checks drawn on the closed accounts:

- **TeleCheck**®—1-800-710-9898 or 927-0188
- **Certegey, Inc.**—1-800-437-5120
- **International Check Services**®—1-800-631-9656.

- 3) File a police report and obtain a copy for submission to credit reporting agencies, creditors, and others.
- 4) Contact the Federal Trade Commission to report the theft and obtain further guidance as to how to protect yourself.

## Identity Fraud

- [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)
  - 1-877-IDTHEFT (438-4338)
  - Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.
- 5) Contact the U.S. Postal Service if you know or suspect your mail has been stolen.
  - 6) Keep detailed records of any theft of your identity and of your activities to resolve the theft, including logs of the following:
    - The date, time, and amount of any unauthorized activity on your accounts;
    - The date, time, duration, and cost of any phone calls; and
    - The date and cost of any mailings.

BANK OF WALKER COUNTY



While Pat settled in for a quiet weekend at home...

## Identity Fraud

Her good name drove off in a new sports car



We i.d. because we care

## What is fraud?

It's the fastest-growing crime in the U.S., costing its victims over \$475 million a year, according to the Federal Trade Commission. Yet, it happens so quietly, most people don't realize they've been victimized until months later. Identity theft—or fraud—occurs when someone uses your personal information without your permission to make illegal purchases, withdrawals, or open accounts. This can damage your credit rating and reputation.

## What are we doing to prevent fraud?

After September 11, legislation was passed to help prevent fraud. Evidence shows that credit card, debit card, and similar fraud is a major source of funding for terrorists. To safeguard our nation against terrorists—and to help prevent you from becoming a victim of fraud—all financial institutions are required to more carefully verify the identity of our account owners, loan applicants, trusts, and individuals who purchase investment products.

This means we may ask you additional questions at the time of your transaction. We may also ask you to provide one or more types of identification (ID), such as a driver's license, U.S. taxpayer ID number, or other government-issued document that verifies your nationality or residence. By answering these questions and providing the required forms of identification, you can help us meet the requirements and better protect you against identity theft.

## What happens to the information you provide us?

The new regulations require us to verify the information you provide us using one or more methods. For instance, we may compare your information against public databases of information to verify that it is current and accurate. Any information we obtain is safeguarded according to our Privacy Policy and information-sharing practices—which were provided to you. That way, you can be confident that your personal information remains secure as we work toward preventing all forms of fraud.

## What else can you do to prevent fraud?

- Keep your credit cards, debit cards, personal identification numbers (PINs), checks, social security number, driver's license number, and other personal information in a safe place.
- Keep deposit and withdrawal slips and credit and debit card receipts where they will be safe, and always shred them first before they're disposed.
- Before disposing of credit card solicitations, credit card statements, financial institution statements, utility bills, insurance information, medical bills, and investment updates, shred them first.
- Don't put your trash out until shortly before it will be picked up.
- Don't put mail in your curb side mailbox until shortly before it will be picked up.
- Take your mail out of your curb side mailbox as soon as possible after it's delivered. And, if you're traveling, have the U.S. Postal Service hold your mail or have someone you trust pick it up daily.
- Limit the information on your checks, and don't carry around any more credit or debit cards than necessary.

- Don't give any of your personal information to anyone in person, over the telephone, or over the Internet, unless you have a very good reason to trust them.

- Don't give any of your personal information in response to an unsolicited e-mail claiming to be from your financial institution or some other highly credible source. This is a technique referred to as "phishing." Be sure to validate the request before providing the information (for example, contact the customer service telephone number on your account statement to ask about the request).

- Don't give any of your personal information to any web sites that don't use encryption or other secure methods to protect it.

- Use a firewall if you have a high-speed Internet connection. This software can be purchased on-line or from most software retailers.

- Don't use PINs or other passwords that are easy to guess (such as family birth dates or your pet's name).

- Examine your credit card, debit card, and bank statements immediately when you receive them to determine whether there are any unauthorized transactions. Report any that you find immediately to the financial institution.

- Make a prompt inquiry if bills or statements are not received in a timely manner—this could mean they are being diverted by an identity thief.

- Obtain copies of your credit report annually from each of the three major credit reporting agencies (Equifax®, 1-800-685-1111; Experian®, 1-888-397-3742; TransUnion®, 1-800-888-4213) to make sure they're accurate.

- You may also wish to do the following:

- Request to not receive any further preapproved offers of credit by calling 1-888-5-OPT-OUT.

- Ask to be removed from national direct mail lists by writing to the DMA Mail Preference Service at P.O. Box 643, Carmel, NY 10512, or going online to [www.the-dma.org/consumers/offmail-ndlist.html](http://www.the-dma.org/consumers/offmail-ndlist.html). Include your name and address.

- Register with the National Do Not Call Registry by calling 1-888-382-1222 or going online at [www.donotcall.gov](http://www.donotcall.gov).