

Identity Theft: Reduce Your Risk

Account fraud and identity theft are serious problems. While you can't completely prevent identity theft, you can minimize your risk by managing your personal information wisely.

At IBM Southeast FCU we are concerned about the safety of our Members. Working together, we'll ensure that you enjoy a secure relationship with your Credit Union and shield you from the threat of account fraud or identity theft. This is all part of what makes us unique; a tradition of caring for our Members backed by the kind of service that gives you a real feeling of security.

What is Identity Theft?

Identity theft occurs when someone uses your name or personal information, such as your Social Security number, driver's license number, credit card number, telephone number or other account numbers, without your permission. Identity thieves use this information to open credit accounts, bank accounts, telephone service accounts, and make major purchases—all in your name. Information can be used to take over your existing accounts, or to open new accounts. Identity theft can result in damage to your credit rating and denials of credit and job offers.



What makes IBM
Southeast Employees' Federal
Credit Union unique?

Our personalized service.
Without it, we would be just another
financial institution.

Visit
www.ibmsecu.org
For eOffers

Please note IBM Southeast EFCU is not affiliated with the FTC or the listed credit agencies and cannot guarantee the accuracy or effectiveness of the information they provide. Information was prepared with the assistance of the Privacy Rights Clearinghouse, the Identity Theft Resource Center and the Federal Trade Commission. This document may be reproduced for non-profit educational purposes.



**IBM Southeast Employees'
Federal Credit Union**

Your time. Your money. Your future.®

P.O. Box 5090, Boca Raton, FL 33431-0890



Security
Tips You Can
Identify With

Protect Your Identity

While there is no guarantee that your identity will never be stolen, there are steps you can take to minimize the risk:

- ◆ Do not give out your Social Security number to people or companies that you do not know.
- ◆ Before disclosing any personal information, make sure you know why it is required and how it will be used.
- ◆ Shred information you no longer need that contains personally identifiable information and account numbers. For example, credit card receipts, billing statements and pre-approved credit offers should be shredded before you discard them.
- ◆ Guard your mail from theft. Promptly remove your incoming mail from your mailbox and place outgoing mail in post office collection boxes. Install a locking mailbox if mail theft is a problem in your neighborhood.
- ◆ Keep the personal information you have at home and at work in a safe place.
- ◆ Do not carry extra credit cards, your birth certificate or passport, or other cards that display your Social Security number in your wallet or purse, except when necessary.
- ◆ Create unique passwords and personal identification numbers (PINs) and avoid using easily available information such as mother's maiden name, date of birth, or the last four digits of your Social Security number.
- ◆ Use passwords on your banking and brokerage accounts.
- ◆ Get a copy of your credit report from each of the three major credit reporting agencies at least once a year. Review the reports to be sure no one else is using your identity to open new accounts or to use your existing accounts.

ATM and Check Card Tips

- ◆ When using an ATM or point-of-sale terminal, make sure that anyone waiting to use the ATM after you cannot see you entering your PIN or transaction amount. Be sure to take your receipt with you.
- ◆ When using your check card for purchases, check your receipt to make sure the correct amount has been debited. Make sure you have your card when your transaction is complete.

The three major credit report bureaus are:

- ◆ **Equifax**
Order Credit Report: 800-685-1111
Report Fraud: 800-525-6285
www.equifax.com
- ◆ **Experian**
Order Credit Report: 888-397-3742
Report Fraud: 888-397-3742
www.experian.com
- ◆ **Trans Union**
Order Credit Report: 800-888-4213
Report Fraud: 800-680-7289
www.tuc.com

If You Are a Victim of Identity Theft

- ◆ Contact the fraud department of one of the three major credit bureaus (the other two will be automatically notified). Request that a "fraud alert" be placed on your file and include a statement that creditors must get your permission before any new accounts are opened in your name. Get a copy of your credit report from each credit bureau so that you can dispute any inaccurate information. Check your reports at least every six months.
- ◆ Contact all the creditors involved. Let them know that your accounts may have been used without your permission, or that new accounts have been opened in your name. If your accounts have been used fraudulently, ask that new cards and account numbers be issued to you. Check your billing statements carefully and report any fraudulent activity immediately. Many banks and creditors will accept the Federal Trade Commission's (FTC) "ID Theft Affidavit" available at www.consumer.gov/idtheft, to dispute the fraudulent charges.
- ◆ File a police report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- ◆ Contact the Federal Trade Commission. The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338), or online at www.consumer.gov/idtheft.
- ◆ If an identify thief has stolen your mail, falsified change-of-address forms, or obtained your personal information through fraud conducted by mail, report it to your local Postal Inspector. The United States Postal Inspection Service (USPIS) - www.usps.gov/websites/depart/inspect - is the law enforcement arm of the U.S. Postal Service responsible for investigating cases of identity theft. Visit the USPIS Web site to locate the USPIS district office nearest you, or call your local U.S. Post Office.
- ◆ The Social Security Administration (SSA) Office of the Inspector General investigates cases of identity theft. To report your Social Security number stolen or misused, contact the SSA Fraud Hotline by phone at (800) 269-0271, by fax at (410) 597-0118, by e-mail at oig.hotline@ssa.gov, or by mail to SSA Fraud Hotline, P. O. Box 17768, Baltimore, MD 21235.

