



# McCoy Federal Credit Union

*Your Full-Service Community Credit Union*

## **PROTECTING YOUR IDENTITY**

Enclosed please find information regarding identity theft and what you can do to prevent it from happening to you. Please read this information carefully. You may also obtain information on this subject from the Federal Trade Commission at: [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)

We also ask that you change your account number with McCoy Federal Credit Union. We realize this may seem burdensome but it is meant to give you peace of mind. Please visit one of our offices as soon as possible to complete the paperwork necessary to assign a new account number. All authorized signers on the account must be present and provide us with a valid form of identification containing both a picture and a signature, such as a driver's license.

At that time we will place an order for checks, at no cost to you (McCoy Custom Creations only), we will assign the starting check number according to your needs, and where applicable we will order new Visa Debit Cards and or McCoy credit cards. We will also ask you to review your current account for unauthorized activity. Your new account number will reflect the fact that you have been a valued member of McCoy Federal Credit Union from your original membership start date.

We ask that you bring this letter with you when you visit our office.

Please know that McCoy Federal Credit Union takes your privacy very seriously. We ask that you take these steps to assist us in protecting your most valuable asset, your identity.

Sincerely,

McCoy Federal Credit Union



# McCoy Federal Credit Union

Your Full-Service Community Credit Union

## IDENTITY THEFT REDUCE YOUR RISK

### WHAT IS IDENTIFY THEFT?

Identify 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.

### HOW DOES IDENTITY THEFT HAPPEN?

Identity theft commonly begins with the loss or theft of a wallet or purse. But there are many other ways that criminals can get and use your personal information in order to commit identity theft. The following are some examples:

**EXAMPLE #1** - One evening you sit down to pay your monthly bills. You write the checks, toss the statements in the trash and put the container out on the curb for the morning's trash pick-up. While you sleep, "dumpster-drivers" go through your trash looking for the papers you've thrown away. They discover a gold mine of information that can be used for fraudulent purposes - your name, address, phone number, utility service account numbers, credit card numbers, and your Social Security number.

**EXAMPLE #2** - You receive an email message from what appears to be your Internet Service Provider (ISP). The message requests that you update the information they have on file about you – your name, credit card number, bank account number, etc. – by replying to the email or going to a specific Web site address to provide the information. However, neither the message nor the Web site address is from your ISP. They belong to someone who wants to get your information to steal your identity.

### PROTECT YOUR IDENTIFY

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 not use your existing accounts.

### IF YOU'RE A VICTIM

- Contact the fraud departments of the three major credit bureaus. 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.

You can contact the three major credit bureaus at the following:

- 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

- **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 "ID Theft Affidavit" available at [www.consumer.gov/idtheft](http://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 identify 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); by mail, Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, DC 20580; or online at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft). Also request a copy of the publication, ID Theft, When Bad Things Happen to Your Good Name.
- **Keep a record of your contacts.** Start a file with copies of your credit reports, the police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties. Follow up all phone calls in writing and send all correspondence certified, return receipt requested.

These additional resources may also be of help.

### NON-PROFIT ORGANIZATIONS

Privacy Rights Clearinghouse, 3100 5th Ave., Suite B, San Diego, CA 92103  
619-298-3396 / Email: [prc@privacyrights.org](mailto:prc@privacyrights.org) / [www.privacyrights.org](http://www.privacyrights.org)

Identify Theft Resource Center, P.O. Box 36833, San Diego, CA 92196  
Email: [voices123@att.net](mailto:voices123@att.net) / [www.idtheftcenter.org](http://www.idtheftcenter.org)

### FEDERAL GOVERNMENT AGENCIES

Federal Bureau of Investigation / [www.fbi.gov/contact/fo/norfolk/ident.htm](http://www.fbi.gov/contact/fo/norfolk/ident.htm)  
FBI Internet Fraud Complaint Center / [www.ifccfbi.gov](http://www.ifccfbi.gov)

Federal Trade Commission, Identify Theft Clearinghouse,  
600 Pennsylvania Ave., N.W., Washington, DC 20580  
1-877-IDTHEFT (438-4338) / [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft)

Social Security Admin., SSA Fraud Hotline, P.O. Box 17768, Baltimore, MD 21235  
/ 1-800-269-0271 / email: [oig.hotline@ssa.gov](mailto:oig.hotline@ssa.gov)

U.S. Postal Inspection Service / [www.usps.gov/websites/depart/inspect](http://www.usps.gov/websites/depart/inspect)

### STATE & LOCAL GOVERNMENT AGENCIES -

Contact your State Attorney General's office or local consumer protection agency to find out whether your state has laws related to identify theft.

### IDENTIFY THEFT PREVENTION TIPS:

- Safeguard your personal information.
- Do not share personal information with unknown person or companies.
- Carry with you only the information you need.
- Order and review a copy of your credit report at least once a year.
- Shred documents containing sensitive information before discarding.

### IF YOU BECOME A VICTIM:

- Contact McCoy Federal Credit Union fraud department
- Contact all the creditors involved.
- File a police report.
- Contact the Federal Trade Commission.
- Keep a record of your contacts.