COLUMBUS METRO FEDERAL CREDIT UNION

IDENTITY THEFT: TIPS FOR PREVENTION & RECOVERY

WHAT IS IDENTITY THEFT?

Identity theft is the use of your personal financial information (Social Security Number, bank or credit union account numbers, credit card information, etc.) to steal from your existing accounts or open new accounts in your name.

WHY SHOULD I BE CONCERNED?

The impact of identity theft on an individual is significant:

- The average identity thief amasses *$10,000 in charges* before the theft is noticed.
- A victim spends an average of *600 hours* restoring his or her reputation.
- Since 1999, an estimated *27 million Americans* have been victims of some sort of identity theft.

WHAT CAN I DO TO PREVENT IDENTITY THEFT?

- Don't put outgoing mail in your home mailbox with the flag up. Instead, drop your mail off at the post office or deposit it in a secure US Postal Service drop box.
- Know when your monthly credit card and bank statements arrive and be sure to review them each month. If they don't arrive on time, call the company. If you have computer access, consider signing up for e-statements.
- Reduce the amount of junk mail and telemarketing calls you receive.
  - When you open a new account, inform the company that you do not want them to share your information with other businesses.
  - Call 888.5OPTOUT (888.567.8688) or visit www.optoutprescreen.com and ask that the three credit bureaus not sell or share your information.
  - Write to the Direct Marketing Association and opt out of most junk mail at Mail Preference Service, Direct Marketing Association, PO Box 643, Carmel, NY 10512.
  - Register your home and cell phone numbers with the National Do Not Call Registry at 888.382.1222 or www.donotcall.gov.
- Don't give out information over the phone if you didn't initiate the call. The same goes for emails requesting personal information, including those that appear to be from legitimate businesses.
- Don't carry your Social Security card with you, and question anyone who says they need your SSN.
- Use passwords that can't be easily guessed. This goes for ATM, debit and credit card PINs, computer passwords, etc.
- Don't write the PIN for an ATM, debit or credit card on the card itself.
- Don't shop online without confirming that the site is secure. Look for the padlock icon at the bottom of the page, and check for an 'S' in the URL on the address bar (i.e. HTTPS://).
- Use anti-spyware and anti-virus protection on your computer, and be sure to update it regularly. If you have a broadband connection (DSL or cable), use a personal firewall. Update your operating system (Windows, for example) regularly.

continued

WHAT CAN I DO TO PREVENT IDENTITY THEFT? continued

- Monitor your credit reports. You are entitled to a free credit report from each of the three major credit reporting agencies each year. (A good way to monitor your credit is to order one free credit report every four months. In other words, order your free report from TransUnion in January. In May, order your free report from Experian. Then in September, order your free report from Equifax. The following January, start the cycle over again.) To order your free reports:
  - Call 877.322.8228
  - Visit www.annualcreditreport.com
  - Write the Annual Credit Report Service, PO Box 105281, Atlanta, GA 30348-5281.

HOW WOULD I KNOW IF I HAVE BEEN AN IDENTITY THEFT VICTIM?

Signs of identity theft include:

- Failing to receive bills or other mail.
- Receiving credit cards you didn't apply for.
- Being denied credit or being offered less favorable terms (such as a higher rate) than in the past.
- Getting calls or letters from debt collectors or businesses about merchandise or services you didn't purchase.

WHAT SHOULD I DO IF I HAVE BEEN A VICTIM OF IDENTITY THEFT?

- Contact the Federal Trade Commission at 877.438.4338 or www.consumer.gov/idtheft and request the booklet, *When Bad Things Happen To Your Good Name.*
- Contact one of the three major credit reporting agencies and ask that a fraud alert be placed on all of your accounts. The three agencies (with the phone numbers for their fraud departments) are Experian (888.397.3742), TransUnion (800.680.7289) and Equifax (888.766.0008).
- Contact credit card issuers and your credit union or bank. If your accounts have been compromised, close the affected accounts and open new ones.
- File a report with your local police or sheriff's department.
- Register with the Ohio Identity Theft Verification Passport Program by contacting the Ohio Attorney General's Office at 888.MYIDFORME (888.694.3463) or www.ag.state.oh.us.

WHAT IS COLUMBUS METRO DOING TO PROTECT MY IDENTITY?

Our goal is to protect your privacy and keep your personal information safe. To that end, we use the best available technology and we train all of our employees to practice sound data protection procedures. Some of the protections we have in place include:

- **Firewall Protection.** Our computer systems are protected by a firewall that prevents online attacks, break-ins and snoopers. The firewall is subject to regular intrusion testing and its software is updated frequently.
- **Encryption Technology.** When you bank online with us, our encryption technology scrambles your information so that it cannot be intercepted as it passes across the Internet.
- **Privacy Policy.** Our employees and our third-party vendors are bound by our Privacy Statement. We do not sell your personal financial information to third parties, nor do we allow our vendors to do so.
- **Privacy-Protecting Services.** We offer a number of electronic services — MetroWeb, MetroWeb Bill Pay and e-statements, for example — that reduce the likelihood that your account information can be compromised. Ask us for more information on any of these services.

If you have any questions or concerns, please contact us at 614.239.0210 or 800.986.3876
To report a lost or stolen Visa® card after hours, call 800.991.4961
To report a lost or stolen MasterMoney® Check Card after hours, call 800.528.2273