CREDIT UNION

Caring for your financial health.

Identity Theft Red Flag Tips

You Can Minimize Your Risk

In the course of a busy day, you may write a check at the grocery store, charge tickets to a ball game, rent a car, mail your tax returns, call home on your cell phone, order new checks, or apply for a credit card. Everyday transactions that you may never give a second thought to are an identity thief's bread and butter. Each of these transactions requires the sharing of personal information: your bank and credit card account numbers; your income, Social Security number and name, address and phone numbers, to name a few. While you can't prevent identity theft, you can minimize your risk by managing your personal information wisely.

Here are Some Tips to Help You Minimize the Risk.

By managing your personal information wisely, cautiously and with an awareness of the issue, you can help guard against identity theft:

- Before you reveal any personally identifying information, find out how it will be used and whether it will be shared with others. Ask if you have a choice about the use of your information: can you choose to have it kept confidential?
- Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time. A missing credit card bill could mean an identity thief has taken over your credit card account and changed your billing address to cover his tracks.
- Guard your mail from theft. Deposit outgoing mail in post office collection boxes or at your local post office. Promptly remove mail from your mailbox after it has been delivered. If you're planning to be away from home and can't pick up your mail, visit www.USPS.com or call the U.S. Postal Service at 1-800-275-8777 to request a vacation hold. The Postal Service will hold your mail at your local post office until you can pick it up.
- Put passwords on your credit card, credit union, and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.
- Minimize the identification information and the number of cards you carry to what you'll actually need.
- Do not give out personal information on the phone, through the mail or over the Internet unless you have initiated the contact or know who you're dealing with. Identity thieves may pose as representatives of banks, Internet service providers and even government agencies to get you to reveal your SSN, mother's maiden name, financial account numbers and other identifying information. Legitimate organizations with whom you do business, including KH Credit Union, have the information they need and will not ask you for it.
- Keep items with personal information in a safe place. To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, bank checks and statements that you are discarding, expired charge cards and credit offers you get in the mail.
- Be cautious about where you leave personal information in your home, especially if you have roommates, employ outside help or are having service work done in your home.
- Find out who has access to your personal information at work and verify that the records are kept in a secure location.
- Give your SSN only when absolutely necessary. Ask to use other types of identifiers when possible.

- Don't carry your Social Security card; leave it in a secure place.
- Order a copy of your credit report from each of the three major credit reporting agencies every year. To ensure it is accurate and includes only those activities you've authorized. You are eligible for a free credit report from each credit bureau one time per year. (The law allows credit bureaus to charge you up to $10.50 for a copy of your credit report thereafter.) However, if you have been denied credit in the last 60 days, you can also request a free copy of your report.

Keeping Your Personal Information Secure Online

Know who you share your information with. Store and dispose of your personal information securely.

- Be Alert to Impersonators - Make sure you know who is getting your personal or financial information. Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or know who you're dealing with. If a company that claims to have an account with you sends email asking for personal information, don't click on links in the email. Instead, type the company name into your web browser, go to their site, and contact them through customer service. Or, call the customer service number listed on your account statement. Ask whether the company really sent a request.
- Safely Dispose of Personal Information - Before you dispose of a computer, get rid of all the personal information it stores. Use a wipe utility program to overwrite the entire hard drive. Before you dispose of a mobile device, check your owner's manual, the service provider's website, or the device manufacturer's website for information on how to delete information permanently, and how to save or transfer information to a new device. Remove the memory or subscriber identity module (SIM) card from a mobile device. Remove the phone book, lists of calls made and received, voicemails, messages sent and received, organizer folders, web search history, and photos.
- Encrypt Your Data - Keep your browser secure. To guard your online transactions, use encryption software that scrambles information you send over the internet. A "lock" icon on the status bar of your internet browser means your information will be safe when it's transmitted. Look for the lock before you send personal or financial information online.
- Keep Passwords Private - Use strong passwords with your laptop, credit, bank, and other accounts. Be creative: think of a special phrase and use the first letter of each word as your password. Substitute numbers for some words or letters. For example, "I want to see the Pacific Ocean" could become 1W2CtPo.
- Don't Overshare on Social Networking Sites - If you post too much information about yourself, an identity thief can find information about your life, use it to answer 'challenge' questions on your accounts, and get access to your money and personal information. Consider limiting access to your networking page to a small group of people. Never post your full name, Social Security number, address, phone number, or account numbers in publicly accessible sites.

Keeping Your Devices Secure

- Use Security Software - Install anti-virus software, anti-spyware software, and a firewall. Set your preference to update these protections often. Protect against intrusions and infections that can compromise your computer files or passwords by installing security patches for your operating system and other software programs.
- Avoid Phishing Emails - Don't open files, click on links, or download programs sent by strangers. Opening a file from someone you don't know could expose your system to a computer virus or spyware that captures your passwords or other information you type.
- Be Wise About Wi-Fi - Before you send personal information over your laptop or smartphone on a public wireless network in a coffee shop, library, airport, hotel, or other public place, see if your information will be protected. If you use an encrypted website, it protects only the information you send to and from that site. If you use a secure wireless network, all the information you send on that network is protected.
- Lock Up Your Laptop - Keep financial information on your laptop only when necessary. Don't use an automatic login feature that saves your user name and password, and always log off when you're finished. That way, if your laptop is stolen, it will be harder for a thief to get at your personal information.
- Read Privacy Policies - Yes, they can be long and complex, but they tell you how the site maintains accuracy, access, security, and control of the personal information it collects; how it uses the

information, and whether it provides information to third parties. If you don't see or understand a site's privacy policy, consider doing business elsewhere.

If You Are a Victim of Identity Theft; Do These Five Things Immediately!

1. Contact the fraud departments of each of the three major credit bureaus and report that your identity has been stolen. Ask that a "fraud alert" be placed on your file and that no new credit be granted without your approval.
2. For any accounts that have been fraudulently accessed or opened, contact the security departments of the appropriate creditors or financial institutions. Close these accounts. Put passwords (not your mother's maiden name) on any new accounts you open.
3. Contact the Federal Trade Commission (FTC) at IdentityTheft.gov
4. File a report with your local police or the police where the identity theft took place. Get a copy of the report in case the bank, credit card company, or others need proof of the crime later on.
5. Sign up or use benefits of KHCU's Perks Checking Account for a minimum monthly fee that will give you access to identity theft protection.

Information for this article was obtained from the Federal Trade Commission (FTC). For more information, visit the FTC Identity Theft website at www.consumer.gov/idtheft

	Equifax	**Experian**	**Trans Union**
Address	P.O.Box 740241 Atlanta, GA 30374-0241	P.O.Box 2104 Allen, TX 75013	760 Sproul Rd. P.O. Box 390 Springfield, PA 19064-0390
Order Credit Report	1-800-685-1111	1-888-397-3742	1-800-916-8800
Report Fraud	1-800-525-6285	1-888-397-3742	1-800-680-7289