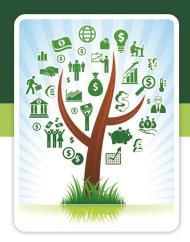
## ARBOR ADVICE

Helpful financial tips provided by Arbor Bank

## **Protect Yourself from Tax-Refund Fraud**

February 13, 2013



Tax season has officially begun. Even if you're not ready to start preparing your taxes, you need to start thinking about protecting your identity. Identity thieves are very active during tax time and can to use your information to file a fraudulent return to claim your refund. The IRS has stepped up its efforts to protect taxpayers from identity theft; however, taxpayers need to take their own steps to protect their identity and guard against fraud during tax season.

Guard your Social Security number. Never carry your Social Security card or number with you. Be hesitant about giving out your number when asked while conducting business—ask the agency or organization you're working with if they can continue without it. There are some times when your Social Security number will be required, such as an application for credit or a license.

Monitor your mailbox. Make sure you receive all of the tax forms you're expecting. If you fail to receive a form, contact that company or financial institution to find out if and when it was mailed. If you suspect that any of these forms were stolen, contact the IRS Identity Protection Specialized Unit at 1-800-908-4490 extension 245.

**Protect your refund.** If you file your tax return by mail, use certified mail from the U.S. Postal service to confirm that your return was received. Opt to have your tax refund directly deposited into your account to avoid a lost or stolen check.

**Ignore emails from the IRS.** The IRS does NOT send taxpayers e-mails or text messages. Do not reply to e-mails or messages from the IRS and never open any attachments or links. Forward all fraudulent e-mails to phishing@irs.gov.

Be wary of people claiming to be IRS agents. Don't reveal any personal information if someone calls and claims to be from the IRS. Instead, call the IRS at 1-800-829-1040 to see if an agent has a legitimate need to contact you first.

Store sensitive information in a secure place. Store paper tax forms in a locked safe or safe-deposit box. Electronic forms should be stored on a password-protected drive or disk—make sure to use strong passwords that include upper and lowercase characters, numbers and symbols. Never store tax files or any personal information on a cloud or internet drive.

Be picky about your preparer. Many fraudsters front as tax-preparation companies and offer to review returns for inaccuracies, but then steal your information and have the ability to redirect your refund. You can verify the status of a preparer's license with the Better Business Bureau and IRS Office of Professional Responsibility.

Before handing over any personal information, ask the tax preparer how your information will be stored and what his or her privacy policy is. This will help you feel more secure and will alert a less-than-reputable preparer that you're on the ball. Most important, scrutinize your prepared return and don't sign it if it is incomplete or if the preparer has failed to sign it.







