

Ferry's Bookkeeping, Etc. LLC

I want to share with you some specific action items that I recommend you do to protect yourself from identity theft.

Identity theft occurs when a thief uses your personal financial information without your permission to commit a crime or fraud. They may find and use your credit card number on a bill you have thrown out or a stray receipt. They may use a device to capture your card number when you use it. And they may even fill out a change of address card and divert your statements.

Between 500,000 and 700,000 individuals are seriously affected by identity theft in the United States each year. Some victims have spent a lot of money and time repairing their credit rating and financial status. Other individuals have been unable to purchase cars, houses, or other items when they needed them because of their “new” and unwelcome credit rating.

We recommend you do as many of the items below as possible to protect yourself.

- **Protect Your Signature.** Never publish your real signature on your web site, in an email signature file, or anywhere else publicly. If you throw out papers with your signature on it, shred them.
- **Take Care with Financial Documents.** Keep a shredder by every trash can where you throw out papers. Take a good look at every paper you throw out and shred every paper that has your Social Security number, credit card number, driver's license number, or any other personal identifying number or information. This will reduce the risk of dumpster diving – where thieves go through your trash to find personal information.
You might be surprised at which papers have identifying information on them. You might need to shred mail that you don't even want to open – for example, credit card applications. Please be careful to inspect all papers or just make a systematic rule to shred everything.
- **Protect Your Records.** Be careful who has access to your financial records, even in your own house. If you have lots of house guests, teenagers with numerous friends, or neighbors over all the time, you have a slight risk of exposure. Keep your papers all in one place, and if possible, lock them up for safekeeping and limited access to people you trust. Don't forget about the papers you leave out on top of your desk or in a mail stack.
- **Protect Your Computer.** Do you have financial information on your computer? Password-protect your financial files, and keep your password in a private, safe place.
- **Be Web Savvy.** Use good judgment when entering credit cards on web sites of businesses you don't know or when presenting your card to a business that looks questionable. This will reduce the risk of skimming, where thieves posing as merchants steal your card number as they enter it in their device.
- **Be Email Savvy.** Never enter your credit card number in an email to someone. Never reply to an email that requests your personal information. If you think the email is real, go to your bank branch in person to check it out. This will reduce the risk of phishing, where the thief poses as a bank to get your information.

Ferry's Bookkeeping, Etc. LLC

- **Be Phone Savvy.** If someone calls you and later asks for your personal information, be wary. It could be a setup, and it's very easy to fall for. The caller will get you engaged in solving a big problem with your account and you could let your guard down. Don't! If there's a question in your mind about whether it's real or not, call the business using the phone number on the back of the credit card or in the phone book.
- **Be Discreet.** Watch how you hold your credit card in a public place such as a line at the supermarket (cover the numbers). Don't say your credit card number in public, and don't repeat it on a cell phone. This is a low risk, but cell phone conversations are easily intercepted.
- **Stay Vigilant with Statements.** Make sure you receive your statements on a timely basis. If a statement is a few weeks late, follow up with the institution to find out why. Better yet, convert to online statements. This will avoid the risk of a thief changing your address and diverting the statements.
- **Keep Track of Your Reports.** Monitor your accounts, bank accounts, credit cards, and credit reports regularly.
- **Spread the Word.** Educate everyone in your household about these ideas so that they are fully implemented.

If you discover fraudulent activity on your accounts, there are four things to do **immediately** (time is of the essence):

- Place a fraud alert on your accounts.
- Close your affected accounts.
- File a police report.
- File a complaint with the Federal Trade Commission (FTC).

The FTC has more information on their web site to help protect you from becoming a victim of identity theft.

<http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html>

If you have any questions about these action items, please call our office. We would love to help you. April 29, 2008