

The Daily Union
Saturday, March 31, 2018
Title: Identity Theft Revisited

In the March 10 Daily Union, I shared an article I had written about consumer protection and resources. In response to that, I have received some requests asking for more information about identity theft. For that reason, I am re-sharing an in-depth article I wrote about the topic some time back. The information shared still holds true today as identity theft continues to be a common complaint to the Federal Trade Commission (FTC).

The FTC has been reaching out to educate consumers through various organizations, like K-State Research and Extension to help spread the word about this growing concern. The FTC shares that "Identity theft occurs when someone steals your personal information and uses it without your permission." This could occur in a variety of ways including tax-related identity theft, child identity, or medical identity theft just to name a few.

Examples of how tax-related identity theft occurs includes when a person uses your Social Security Number to get a job or claim your tax refund. Among other examples, child identity theft is often the result of a thief trying to open a credit card, apply for government assistance or attempt to rent an apartment. Medical identity theft occurs when someone tries to use your health insurance card and related information to see a doctor or make a claim with your insurance provider. Identity theft creates a snowball effect of negative experiences and often people are unaware that their identity has been stolen until they get an unexpected letter in the mail or a surprise phone call from their banking institution or insurance company. Common ways in which consumers become aware that they may be experiencing identity theft which include: unexplainable withdrawals from their bank account; use of checks being declined at stores; claims on a health insurance company summary report that are incorrect; debt collectors contact the consumer about debts they did not create; or the IRS contacts you that more than one tax return was filed under the consumer names, to name a few.

There are several things a person can do to help prevent this situation or to catch the outcomes early enough to limit or prevent long-term credit damage for the consumer. First, review your credit report on a regular basis. You can get one free credit report from each of the three major credit bureaus each year. If you request a report from a different bureau every 4 months, you will be able to access this service without expense and keep a close eye on your credit report activities. A secure site to order your credit report is at www.annualcreditreport.com or you can call 1-877-322-8228. Another important step includes taking a close look at the individual charges made to your credit card accounts, transactions in your banking account and medical use summary reports. Shredding paperwork that contains your personal information is

important, as well. Make sure your computer system is secure by using spyware and anti-virus programs, as well as using a firewall. Create secure passwords for your accounts by combining upper and lower case letters with symbols and numbers. This makes it much more difficult for a person to replicate what you have typed into a keypad. Don't respond to e-mail, phone calls, or letters that request your personal information – legitimate companies don't ask for this information this way.

How do thieves access your personal information? This can occur in a variety of ways. Some will rummage through trash to get your personal information off of discarded mail or other documentation. Some will take personal information by stealing mail directly from your mail box. If a person works for a company that has access to your personal information, they may take the information illegally from your records. Another common scam is to contact you via e-mail or phone to encourage you to claim a prize or to offer you a job. They will use this guise in an attempt to collect your personal information directly from you.

What should you do if you suspect that you are a victim of identity theft? There are three key initial steps. First, call one of the three major credit bureaus (Equifax, Experian, or TransUnion) to request that a fraud alert is placed on your report. You do not need to call all three because they are required to report this information to the remaining bureaus. Second, order a report from each bureau to compare the credit activity on each. The format of each company's report varies and comparing the reports side by side will help you identify discrepancies more quickly. Finally, the FTC recommends that you file an Identify Theft Report. You can do this by visiting their website at www.ftc.gov/complaint or by calling 1-877-438-4338. The completed complaint is called an FTC Affidavit which should be taken to the police department in the community you live in or where the theft occurred. You will need to file a police report there, as well. Make sure you keep a copy of the affidavit and police report for your records.

To contact one of the major credit bureaus, their phone numbers are: Equifax (1-800-525-6285; Experian (1-888-397-3742); TransUnion (1-800-680-7289.) For more information about identify theft and its prevention, go to <http://www.consumer.ftc.gov/features/feature-0014-identity-theft> or contact the Geary County K-State Research and Extension office at (785) 238-4161.