Identity Theft – Minimize Your Risk

Data security breaches across the country have resulted in consumers asking how they can protect themselves from becoming victims of identity theft. Identity theft results when your personal information is stolen and used by someone else to open new accounts in your name, access your existing accounts, or to assume your identity in financial and other transactions. While it is not possible to completely eliminate the risk of becoming a victim, there are things you can do to minimize your risk.

- First and foremost, check your credit report at least once a year!! Many people first learn they have been a victim of identity theft when they are turned down for credit because of a poor credit record. When they check their credit report, they discover accounts that they did not open.

  Under the Fair and Accurate Credit Transaction Act (FACTA), you can obtain one free copy of your credit report every 12 months from each of the three major credit-reporting agencies. To access your free report, visit www.annualcreditreport.com or call toll free at 877-322-8228. This is the only official website for obtaining your free report under this law. By staggering your requests one every four months, you will be able to check your report at three different times of the year.

  If you have been denied credit in the past 60 days, have been the victim of identity theft, are unemployed and will be looking for work in the next 60 days, or on public assistance, you are entitled to additional credit reports. Credit bureaus charge about $10 per report for additional credit reports.

- If you are notified that your personal information has been breached or you suspect your information has been breached, it is recommended that you notify the fraud department of at least one of the credit-reporting agencies and request that a fraud alert be placed on your file. They will notify the other credit-reporting agencies and have fraud alerts placed on their files. The fraud alert tells creditors, who request your credit report, that fraud has been associated with your report. Creditors should attempt to contact you to confirm that you actually applied for the credit that generated the credit report. This action should reduce or eliminate any new fraudulent credit accounts from being opened. Be sure to verify with the credit bureaus how long the initial fraud alert will remain on your account and what you need to do to extend it.

  The three major credit-reporting agencies and their contact information follows:

  Experian
  www.experian.com
  888-397-3742 (credit report request)
  888-397-3742 (fraud alert)

  TransUnion
  www.transunion.com
  800-916-8800 (credit report request)
  800-680-7289 (fraud alert)

  Equifax
  www.equifax.com
  800-685-1111 (credit report request)
  800-525-6285 (fraud alert)

- Texas law allows you to ‘freeze’ your credit files by requesting a ‘security freeze.’ A security freeze means that your credit file cannot be provided to anyone (other than your current creditors monitoring current accounts) so that an identity thief is less likely to be able to obtain credit in your name. To request a security freeze, you must make the request in writing by certified mail to each credit-reporting agency. A $10 fee applies to place the security freeze at each credit-reporting agency, and an additional $10 fee applies to lift it in advance of applying for credit in the future. Victims of

identity theft do not have to pay the $10 fee. For more details, see http://www.consumersunion.org/pdf/security/securityTX.pdf.

- GUARD your Social Security Number!! Don't routinely carry your Social Security card with you. Leave it in a safe, secure place at home, and only bring it with you when you need it. Ask these questions when you are asked for your Social Security Number:
  - Why do you need it?
  - How will it be used?
  - How do you protect it from being stolen?
  - What will happen if I don't give it to you?

  The answers to these questions will help you decide whether or not to give it to them or whether or not to do business with them. The decision is yours!
- NEVER give out personal information over the phone, in person, via e-mail or the internet unless you have initiated the contact, you know who you are dealing with, and there is a legitimate need for the information. Financial institutions and businesses will not contact you and ask you to verify account information they already have on file.
- Guard your mail and trash. Shred all documents with personal information before you throw it away – preferably with a crosscut shredder. Always place outgoing mail in a secure post office collection box rather than your own mailbox to prevent your mail from being stolen to obtain your account information. Consider getting a locked mail box or using a post office box for incoming mail.
- Secure your personal information at home. Use a lock box or locked file cabinet. This effort is especially important if you have people working for you in your home or you are having service work done.
- Ask your employer how your personal information is safeguarded. Who has access to it? How is it disposed of?
- Only carry the identification, credit and debit cards, and other account information you need. Would you remember all the things in your purse or wallet if it were stolen?
- Reduce the amount of information, requests, and offers you receive in the mail. To opt out of prescreened credit offers, call 888-567-8688 or visit www.optoutprescreen.com. To remove your name from telemarketing calls, visit www.texasnocall.com and www.donotcall.gov. And to remove your name from direct-marketing lists, visit www.dmachoice.org.
- Use virus protection software and a firewall program on your computer. Never download files or click on links from people you don't know or trust.

For more information on identity theft, visit the following sites:

- Federal Trade Commission at http://www.ftc.gov/bcp/edu/microsites/idtheft/
- Texas Attorney General at www.texasfightsidtheft.gov
- Identity Theft Resource Center at www.idtheftcenter.org
- Privacy Rights Clearinghouse at www.privacyrights.org
- Social Security Administration at www.ssa.gov/pubs/10064.html

This information was prepared by Dr. Joyce Cavanagh, Associate Professor and Extension Family Economics Specialist, and Nancy Granovsky, Professor and Extension Family Economics Specialist, Texas A&M AgriLife Extension Service, Texas A&M System. Revised May 2014.