VALEO FINANCIAL ADVISORS, LLC

Identity Theft
What can you do to protect your identity?

Paul A. Donahue, CFP®, AIF®
padonahue@valeofinancial.com

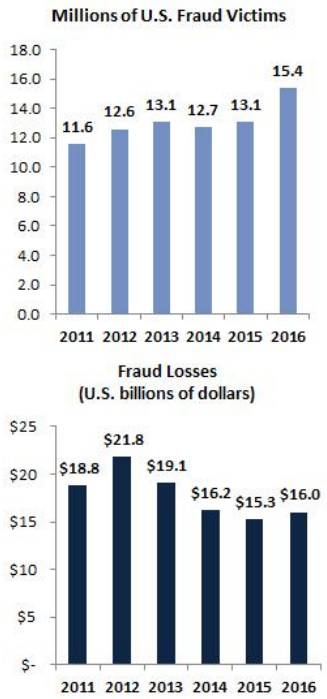
What is identity theft?

- A form of fraud in which one person's identity is used by another to gain access to personal information and other resources including:
  - Bank accounts and credit cards
  - Social Security numbers
  - Internet login information
  - Health insurance
- The victim, normally an unsuspecting individual or corporation, can suffer severe consequences and be held accountable for the misguided actions of others.

Identity Theft Prevention: Best Practices

- Consider obtaining identity theft coverage through your home and auto insurance agent to limit your financial loss.
- "Opt-out" of having your name included on lists used by companies that solicit credit and insurance products at www.optoutprescreen.com.
- Request a free copy of your annual credit report from each credit reporting company at www.annualcreditreport.com once each year.
- Sign up for fraud alerts with the three main credit reporting companies to keep others from opening new credit accounts in your name, and consider requesting a credit freeze to restrict access to your credit.
- Set up alerts for bank and credit cards - many institutions can provide text or email alerts for transactions above a preset threshold.
- Do not click on unknown links or documents if you suspect the e-mail is part of a phishing scam (thieves often impersonate government agencies and banks).
- Phone scams are on the rise – do not reveal personal information if you do not know the identity of a caller. It may be best to let unknown calls go to voice mail. When contacting your bank, or credit card companies, use the phone numbers listed on your statements or on the back of your cards.
- Use caution, thieves attach skimming devices to credit/debit card readers to clone your card data.
- Be aware that debit cards do not offer the same protections against loss as credit cards – an account can be emptied, with little to no hope of restoration.
- For internet purchases, consider prepaid credit cards or on-line payment options, like PayPal or Square, and never use your debit card over the phone.

Total Fraud Victims Reaches Record High and Losses Increase in 2016



Source: Javelin Strategy & Research 2017

How to Strengthen Your Digital Security

- Update your software and apps
- Use lengthy passwords that are different for each site
- Use two-factor authentication
- Consider a password manager such as LastPass
- Encrypt your drives & devices
- Back up data using a back-up drive or service such as Carbonite
- Utilize quality Anti-virus & Malware protection software

VALEO FINANCIAL ADVISORS, LLC

Additional Action Steps to Consider

- Look into having your credit monitored by a company that provides identify theft prevention services such as LifeLock (www.lifelock.com), Identity Guard (www.identityguard.com), Trusted ID (www.trustedid.com) or Family Secure (www.familysecure.com).
- Check out www.creditkarma.com. This site offers a free and easy way to track your credit score over time.
- Track your bank and credit card transactions on a regular basis through www.mint.com or www.yodlee.com
- If you are a victim of identity theft, report it to the FTC at www.identitytheft.gov, file an Identity Theft Report with your local law enforcement agency, and contact one of the credit reporting companies.

What's the difference between a fraud alert and a credit freeze?

- A fraud alert gives you the ability to take out new credit and warns potential creditors about confirming your identity prior to opening a new account. Before a new account can be opened, you will receive a confirmation phone call. These alerts need to be renewed every 90 days and are available at no cost.
- A credit freeze allows you to lock down your credit report to prevent anyone from running a credit report in your name – even you (your existing creditors are exempt from this freeze). You may temporarily lift or permanently remove a credit freeze by calling and/or visiting one of the credit reporting company websites.

How to freeze your credit report?

- You may request a credit freeze directly from each of the credit reporting company websites:

  Equifax: 1-800-525-6285
  https://www.freeze.equifax.com

  Experian: 1-888-397-3742
  https://www.experian.com/freeze

  TransUnion: 1-800-680-7289
  https://annualcreditreport.transunion.com/fa/securityFreeze/landing

- In many states (including Indiana), you can place a credit freeze at no charge. In other states, the charge is typically $10 per credit reporting company.

Helpful Safety Tips

1. Secure your mobile device by taking advantage of security capabilities, software updates and strong passwords
2. Place a security freeze
3. Sign up for account alerts
4. Seek help as soon as fraud is detected
5. Be alert for international transactions

How to Help Aging Parents:

- Talk to them about identity theft and phishing scams.
- Discuss online security, email security and the risks of clicking on links even those coming from names they know.
- Discuss recent telephone and door-to-door scams with them and advise them not to agree to any services from anyone who contacts them. Help them find quality professionals for any repair, insurance or warranty services they may actually need.
- Ask to get involved if they become at high risk.
- Obtain their email account logins and review their email activity.
- Obtain duplicate bank and credit card statements or online access and review for unusual activity.

Identity Theft impact on Minors:

- Children are highly susceptible to identity theft.
- In a study examining 42,232 children and 347,362 adults, children were 51 times more likely to be the target of identity theft.
- Over 10% of children had someone else using their SSN compared with less than 0.2% of adults.
- Types of records involved in child ID theft cases: loan & credit accounts, utility, property, driver's license, and vehicle registration.